ACTA UNIVERSITATIS SZEGEDIENSIS

ACTA JURIDICA ET POLITICA

Tomus LXIII.
Fasc. 7.

HAJDÚ JÓZSEF

A munkavállalók személyes adatainak védelme az EU és a tagállamok jogában, különös tekintettel az elektronikus kommunikációra

SZEGED
2003

Edit

Comissio Scientiae Studiorum Facultatis Scientiarum Politicarum et Juridicarum
Universitatis Szegediensis

LÁSZLÓ BLUTMAN, LÁSZLÓ BODNÁR, JÓZSEF HAJDÚ, ÉVA JAKAB,
JENŐ KALTENBACH, TAMÁS KATONA, JÁNOS MARTONYI,
FERENC NAGY, PÉTER PACZOLAY, BÉLA POKOL, JÓZSEF RUSZOLY,
IMRE SZABÓ, LAJOS TÓTH, LÁSZLÓ TRÓCSÁNYI

Redigit
KÁROLY TÓTH

Nota
Acta Jur. et Pol. Szeged

Kiadja

a Szegedi Tudományegyetem Állam- és Jogtudományi Karának
tudományos bizottsága

BLUTMAN LÁSZLÓ, BODNÁR LÁSZLÓ, HAJDÚ JÓZSEF, JAKAB ÉV
KALTENBACH JENŐ, KATONA TAMÁS, MARTONYI JÁNOS,
NAGY FERENC, PACZOLAY PÉTER, POKOL BÉLA, RUSZOLY JÓZSE
SZABÓ IMRE, TÓTH LAJOS, TRÓCSÁNYI LÁSZLÓ

Szerkeszti
TÓTH KÁROLY

Kiadványunk rövidítése
Acta Jur. et Pol. Szeged

ISSN 0324–6523 Acta Univ.
ISSN 0563–0606 Acta Jur.

I. rész

Bevezetés

Az emberi személyiség meghatározása tudományáganként, világnézetenként és történelmi koronként is állandóan változik. Magánjogi szempontból a jogszabály az ember testi és szellemi működését, integritását és szabadságát védi. Napjainkban a munkát végző ember személyiségi jogainak és magánszférájának a védelme nagyon összetett. Egyrészt védi az ember szellemi értékeit, szubjektumát (például a méltóság, a becsület, a titokvédelem), és védik az emberi személynek az anyagi világban megjelenő testi lényegét is (így pl. a testi épség védelme, kép- és hangvédelem).

A személyiségi jogoknak az ember szubjektumából, egyéniségéből való kiindulásából az következik, hogy e jogok létezésének és meghatározásának első esszenciális eleme, hogy maga az érintett emberi lény – kulturális, szociális, gazdasági, jogi stb. individuum – mit tart saját maga számára fontos és védendő értéknek, mit tekint a saját személyiségi jogának. A második kérdés az, hogy ezekből az igényekből mit ismer el védendőnek az adott társadalom a jogalkotás és a jogszolgáltatás szintjén. „A személyiség a maga alkotó szabadságával a társadalom szempontjából értékes javakat – kultúrértékeket – tud létrehozni, melyekre a társadalomnak szüksége van. Minthogy pedig minden embernek lehet képessége ily érték létrehozására, és senkitől sem lehet az ellenkezőt – legalább pro futuro – kimutatni, ezért a jognak vélelmezni kell minden ember személyiségét, integritását és ezzel egyidejűleg minden ember értékalkotásra való képességét. Ebben az irányban a jognak az a feladata, hogy megóvja a személyiséget minden olyan háborítástól, amely a társadalom szempontjából nem szükséges." [1]

A személyiségi jogok tehát az emberi jogokkal vannak legszorosabb kapcsolatban. Az emberi jogok lényegében az egész emberiség által elfogadott személyiségi jogok is, melyeket nemzetközi és belső normák rögzítenek. A mai személyiségi jog gyökerét a természetjogi szemléletben kell keresnünk, mely a korábbi évezredek isteni eredetű erkölcsi szabályait igyekezett egy általános érvényű emberi joggá átalakítani. Különösen a modern természetjog elvei (pl. jogbiztonság, szabadságjogok) fontosak e tekintetben, amelyek gyakorlatilag az adott kor jogpolitikai elveit és követelményeit tartalmazták.

Összegezve az előbbieket, a *személyiségi jog* fogalmát a következőképpen fogalmazhatjuk meg: a személyiségi jogok az ember értékét, szellemi és fizikai egységét, mindennemű szabadságát védik, koronként és társadalmanként differenciált módon, az egyetemes emberi jogokból és az Alkotmányokból kiindulva.

Egy pragmatikusabb megközelítésben a fenti folyamatot egészíti ki a munkavállalónak, mint speciális helyzetben lévő személynek a jogi védelméből eredő sajátossága. Nagyvonalakban ezt a következőkben foglalhatjuk össze: Alapesetben a munkáltatók tiszteletben tartják a munkavállalók – mint emberek – magánszférához fűződő jogait

[1] BALÁS P. ELEMÉR gondolata 1941-ből; idézi Jobbágyi Gábor: *Személyi és családi jog*. Szent István Társulat, Budapest, 2000, 57. p.

Edit

Comissio Scientiae Studiorum Facultatis Scientiarum Politicarum et Juridicarum Universitatis Szegediensis

LÁSZLÓ BLUTMAN, LÁSZLÓ BODNÁR, JÓZSEF HAJDÚ, ÉVA JAKAB, JENŐ KALTENBACH, TAMÁS KATONA, JÁNOS MARTONYI, FERENC NAGY, PÉTER PACZOLAY, BÉLA POKOL, JÓZSEF RUSZOLY, IMRE SZABÓ, LAJOS TÓTH, LÁSZLÓ TRÓCSÁNYI

Redigit
KÁROLY TÓTH

Nota
Acta Jur. et Pol. Szeged

Kiadja

a Szegedi Tudományegyetem Állam- és Jogtudományi Karának tudományos bizottsága

BLUTMAN LÁSZLÓ, BODNÁR LÁSZLÓ, HAJDÚ JÓZSEF, JAKAB ÉVA, KALTENBACH JENŐ, KATONA TAMÁS, MARTONYI JÁNOS, NAGY FERENC, PACZOLAY PÉTER, POKOL BÉLA, RUSZOLY JÓZSEF, SZABÓ IMRE, TÓTH LAJOS, TRÓCSÁNYI LÁSZLÓ

Szerkeszti
TÓTH KÁROLY

Kiadványunk rövidítése
Acta Jur. et Pol. Szeged

ISSN 0324–6523 Acta Univ.
ISSN 0563–0606 Acta Jur.

I. rész

Bevezetés

Az emberi személyiség meghatározása tudományáganként, világnézetenként és történelmi koronként is állandóan változik. Magánjogi szempontból a jogszabály az ember testi és szellemi működését, integritását és szabadságát védi. Napjainkban a munkát végző ember személyiségi jogainak és magánszférájának a védelme nagyon összetett. Egyrészt védi az ember szellemi értékeit, szubjektumát (például a méltóság, a becsület, a titokvédelem), és védik az emberi személynek az anyagi világban megjelenő testi lényegét is (így pl. a testi épség védelme, kép- és hangvédelem).

A személyiségi jogoknak az ember szubjektumából, egyéniségéből való kiindulásából az következik, hogy e jogok létezésének és meghatározásának első esszenciális eleme, hogy maga az érintett emberi lény – kulturális, szociális, gazdasági, jogi stb. individum – mit tart saját maga számára fontos és védendő értéknek, mit tekint a saját személyiségi jogának. A második kérdés az, hogy ezekből az igényekből mit ismer el védendőnek az adott társadalom a jogalkotás és a jogszolgáltatás szintjén. „A személyiség a maga alkotó szabadságával a társadalom szempontjából értékes javakat – kultúrértékeket – tud létrehozni, melyekre a társadalomnak szüksége van. Minthogy pedig minden embernek lehet képessége ily érték létrehozására, és senkitől sem lehet az ellenkezőt – legalább pro futuro – kimutatni, ezért a jognak vélelmezni kell minden ember személyiségét, integritását és ezzel egyidejűleg minden ember értékalkotásra való képességét. Ebben az irányban a jognak az a feladata, hogy megóvja a személyiséget minden olyan háborítástól, amely a társadalom szempontjából nem szükséges." [1]

A személyiségi jogok tehát az emberi jogokkal vannak legszorosabb kapcsolatban. Az emberi jogok lényegében az egész emberiség által elfogadott személyiségi jogok is, melyeket nemzetközi és belső normák rögzítenek. A mai személyiségi jog gyökerét a természetjogi szemléletben kell keresnünk, mely a korábbi évezredek isteni eredetű erkölcsi szabályait igyekezett egy általános érvényű emberi joggá átalakítani. Különösen a modern természetjog elvei (pl. jogbiztonság, szabadságjogok) fontosak e tekintetben, amelyek gyakorlatilag az adott kor jogpolitikai elveit és követelményeit tartalmazták.

Összegezve az előbbieket, a *személyiségi jog* fogalmát a következőképpen fogalmazhatjuk meg: a személyiségi jogok az ember értékét, szellemi és fizikai egységét, mindennemű szabadságát védik, koronként és társadalmanként differenciált módon, az egyetemes emberi jogokból és az Alkotmányokból kiindulva.

Egy pragmatikusabb megközelítésben a fenti folyamatot egészíti ki a munkavállalónak, mint speciális helyzetben lévő személynek a jogi védelméből eredő sajátossága. Nagyvonalakban ezt a következőkben foglalhatjuk össze: Alapesetben a munkáltatók tiszteletben tartják a munkavállalók – mint emberek – magánszférához fűződő jogait

[1] BALÁS P. ELEMÉR gondolata 1941-ből; idézi Jobbágyi Gábor: *Személyi és családi jog*. Szent István Társulat, Budapest, 2000, 57. p.

(privacy) és méltóságát (dignity). Ilyenkor a munkáltatót a hagyományos munkaviszony keretei között egyébként elvitathatatlanul megillető ellenőrzési és utasítási jog kerete megfelelő módon és objektív alapon alakul át. A jog nyelvére lefordítva ez azt jelenti, hogy a munkáltatói joggyakorlás nem lesz visszaélésszerű, vagyis nem válik sem a belső, sem pedig a nemzetközi jogi standardokkal mérve jogellenessé, sőt a szigorúan véve jognak nem tekinthető ún. jó munkaerőpiaci standardoknak is megfelel. A munkáltató jogszerű magatartásának a határait alapvetően két tényező befolyásolja: *a)* egyrészt a megfigyelés (ellenőrzés) indokoltsága, másrészt *b)* a munkavállalónak ténylegesen okozott vagy potenciális kár, illetve nem vagyoni kár mértéke. E két nagyon érzékeny tényező – munkáltatót megillető jogok, illetve gazdasági érdekek és a munkavállalói személyiségi jogok – arányosításával alakítható ki a munkáltató magatartásának a jogszerű kerete. Ezt nagyon gyakran ún. nem jogi normákban, mint például kollektív szerződés, munkaszerződés, viselkedési kódex vagy etikai standardok stb. is rögzítik. Fontos megjegyezni, hogy abban az esetben, ha a munkáltató megsérti ezeket a közösen felállított szabályokat, akkor ezzel a magatartásával megszegi az együttműködési kötelezettségből és a rendeltetésszerű joggyakorlásból eredő kötelezettségeit.

A munkavállalókat megillető személyiségi jogok védelmének időbeni alakulását tekintve, megállapítható, hogy az 1970-es évek a személyes adatok gyűjtésével és felhasználásával kapcsolatos intenzív magánélet-védelmi kutatás és jogalkotás kezdeti időszaka volt. Ez a folyamat nem teljesen előzmények nélküli, ugyanakkor az utóbbi évtizedekben jelentős mértékben felerősödött. Számos ország és nemzetközi szervezet hivatalos jelentései tanúsítják, hogy e problémát ma már politikai szinten is komolyan veszik. A különböző tanulmányok arra is rámutatnak, hogy az egymásnak ellentmondó érdekek – munkáltató, munkavállaló, üzleti partnerek, állam stb. – kiegyensúlyozása kényes feladat, és aligha oldható fel egyszer s mindenkorra. Napjainkban a közvélemény és a szakemberek egy része is hajlik arra, hogy a személyiség és a magánszféra védelmének széles köréből leginkább az elektronikus adatfeldolgozás lehetséges következményeire és az abban rejlő kockázatokra összpontosítson. Ez a tendencia minden bizonnyal tovább folytatódik, hiszen az információs társadalom és munkavégzés világában szinte minden egyes adat elektronikusan kerül rögzítésre, illetve feldolgozásra. Ezzel párhuzamosan az is tapasztalható, hogy az egyes országok jogalkotó szervei is leginkább a számítógépekre és számítógépekhez kapcsolódó elektronikus adatfeldolgozáshoz kötődő tevékenységekre vonatkozó jogszabályokat alkottak. Ezzel szemben, más országok a magánélet védelmének általánosabb megközelítését választották, függetlenül az alkalmazott adatfeldolgozási módszertől. Felfogásukban a magánszféra védelmére vonatkozó normatív szabályozás olyan teljes körű, az egyén – fizikai és pszichikai – életterét védő biztosítékokat jelent, amelyek megelőzik a magánélet klasszikus értelemben vett megsértését, mint pl. intim személyes adatok nyilvánosságra hozatalát vagy az azokkal való visszaélést. Ugyanakkor felszínre kerültek a magánszféra védelméhez többé-kevésbé közvetlenül kapcsolódó egyéb védelmi igények is, mint például: *a)* a nyilvántartók azon kötelessége, hogy a közvéleményt az adatkezeléssel kapcsolatos tevékenységről tájékoztassák; *b)* továbbá az adatalanyok joga arra, hogy a rájuk vonatkozó adatokat kiegészíthessék vagy módosíthassák. Megfigyelhető az a törekvés, hogy a magánélet hagyományos értelmezését (miszerint a magánszféra védelmének esszenciája: „a békén hagyatáshoz" való jog) kibővítsék és már nemcsak az egyén, hanem a környezetének az érdekeit is védjék. Ez az összetettebb értelmezés már sokkal inkább „a magánélet és a személyes szabadság" olyan típusú védelmét helyezi előtérbe, amely fogalomba beletar-

tozik az egyén családjának és közvetlen lakókörnyezetének a szuverenitásának a biztosítása. A magánszféra védelme tehát nemcsak közvetlenül a munkavállalóra terjed ki, hanem a munkavállaló egy meghatározott személyes környezetére is.

Visszatérve a fő trend elemzéséhez. Az automatizált elektronikus adatkezelés jogi szabályozása terén talán a magánélet és a személyes szabadságjogok védelme a legvitatottabb kérdés. Annak hogy ez a probléma ilyen széles körben kelt figyelmet, az elsődleges oka talán a számítógépek mindenhol egyre nagyobb mértékben elterjedő használatára vezethető vissza. A személyes adatok feldolgozásában, a tárolás, az összehasonlítás, az összekapcsolás, a kiválasztás és a hozzáférés jelentősen megnövekedett lehetőségei, valamint a számítógépek és a távközlési technikák összekapcsolása, amely lehetővé teszi, hogy személyes adatokhoz földrajzilag szétszórt felhasználók milliói férhessenek hozzá egyidejűleg, és amely ugyancsak megvalósíthatóvá teszi az adatgyűjtés központosítását és komplex országos és nemzetközi adathálózatok létrehozását. Egyes problémák különösen sürgős figyelmet kívánnak, például azok, amelyek a nemzetközi adathálózatok megjelenésével, valamint azzal az igénnyel kapcsolatosak, hogy egyensúly jöjjön létre egyfelől a magánélet védelme, másfelől az információszabadság egymással versengő érdekei között annak érdekében, hogy a modern adatfeldolgozás lehetőségeit a kívánatos mértékig, de az egyén személyiségi jogait nem sértve lehessen kihasználni.

A globalizált munkavégzés és ehhez kapcsolódó adatáramlás keretei között természetes, sőt bizonyos értelemben véve szükségszerű fejlemény, hogy a magánszféra – ezen belül is a munkavállalók magánszférájának - védelme nemcsak a belső (nemzeti) jogokban, hanem a nemzetközi normaalkotás szintjén is megjelent. A mértékadó nemzetközi szervezetek – Európa Tanács, OECD és Európai Közösség – normái közül jelen munkánkban az EU irányelveivel foglalkozunk részletesen. Az egyre inkább globalizálódó gazdaságban valószínűsíthető, hogy az államok feletti normaalkotás szerepe a jövőben tovább növekszik. Például a Magyarország számára is meghatározó Európai Unió szabályozásának zászlóshajóját jelentő 95/46/EC Irányelv alapján történő adatkezelést a következő általános alapelvek szabályozzák: *a)* Szükségesség (necessity); *b)* Célhozkötöttség elve (finality); *c)* Áttekinthetőség (transparency; *ca)* Az adatalany megfelelő információkkal való ellátása, *cb)* A Felügyeleti Szerv értesítési kötelezettsége az automatikus vagy részben automatikus megfigyelési rendszer bevezetése előtt; *d)* Hozzáférhetőség (Right of access; *e)* Jogszerűség (legitimacy; *f)* Arányosság (proportionality); *g)* Pontosság és az adatok megőrzése (accuracy and retention of data) és *h)* Biztonság (security). Ezek feltétlen betartása esszenciális fontosságú a gyakorlat számára.

A dolgozatban ezekkel a kérdésekkel foglalkozunk részletesebben. Áttekintjük a vonatkozó Európai Uniós szabályozást és az EU-s tagállamok, illetve az Európai Gazdasági Térség államainak szabályozási rendszerének azon normáit, amelyek a munkahelyi elektronikus eszközhasználathoz kapcsolódó adatvédelmi és személyiségi jogi kérdésekkel foglalkoznak.

1. Az EU szabályozása

Az Európai Unió – felismerve az egyes államok szabályozásának hiányosságait és az államok védelmi rendszerei között meglévő eltéréseket – elfogadott két irányelvet, amelyben az EU polgárainak adatvédelméről rendelkeztek. Ezek az Európai Telekom-

munikációs Irányelv[2] és az Európai Adatvédelmi Irányelv.[3] Ezek az irányelvek iránymutatásul szolgálnak a tagállamok – és a leendő tagállamok – jogalkotói számára. A második irányelv értelmében és szellemében minden tagállamnak 1998 októberéig el kellett fogadnia az irányelv rendelkezéseit végrehajtó (kiegészítő) saját belső normáit. Az irányelv hatálya az EU-n belül szabadon áramló az EU-s polgárokra vonatkozó személyes információ védelmén kívül kiterjed az uniós polgárok személyes adatainak EU-n kívül történő kezelésére, átvitelére is. Ez a rendelkezés alapvetően megtermékenyítőleg hatott az EU-n kívüli országokra is a tekintetben, hogy a magánszféra védelmét szolgáló jogi normákat fogadjanak el. Egyre több ilyen országgal találkozhatunk.

A fent említett két irányelv széleskörűen védi az EU-s polgárok személyes adatait. A két irányelv nem egyszerűen megismétli a korábban elfogadott adatvédelmi jogi normákat, hanem azokon túlmenve új típusú védelmet alapít. Az Adatvédelmi irányelv harmonizációs mintául szolgál az EU tagállamai számára.[4] A Telekommunikációs irányelv[5] speciális védelmi standardokat állít fel a telefon, digitális televíziózás, a mobilhálózatok és más telekommunikációs rendszer vonatkozásában. A telekommunikációs irányelv az általános speciális viszonyában van az adatvédelmi irányelvvel, vagyis az attól eltérő a telekommunikációs ágazatra jellemző speciális szabályokat tartalmazza. A telekommunikációs irányelv elsősorban a szolgáltatókra vonatkozó kötelezettségeket ír elő. Ezek lényege, hogy a felhasználók kommunikációjában lévő személyiségi jogi elemeket védjék. Az új szabályozásnak olyan kérdéseket kell lefednie, amelyek eddig nem kerültek a jogi szabályozás hatáskörébe. Az adatokhoz való hozzáférés értékesítése és a marketing célú felhasználás szigorúan tilalmazott magatartás. A különböző kommunikációs információ szolgáltatások által összegyűjtött adatokat csak addig lehet tárolni, amíg a címzett egyszer lekéri. Ezt követően meg kell azokat semmisíteni. A fent említett EU-s irányelvekben számos alapelvi jelentőségű szabály található. Például az egyénnek joga van arra, hogy ellentételezés és indoklás nélkül kitérjen az ún. direkt-marketing célból küldött szóróanyagok megválaszolása, illetve a programban való részvétel elől.

Tárgyi hatályát tekintve van átfedés a két irányelv között. Például mindkettőben vannak rendelkezések az elektronikus kommunikáció – beleértve az e-mail-t és az internetet – munkáltatói megfigyelésére.

Az adatvédelmi irányelv különös figyelmet szentel az ún. érzékeny személyes adatok – például egészségügyi vagy az egyén pénzügyi helyzetére vonatkozó információk – védelmére. A jövőben az ilyen típusú adatok kereskedelmi vagy kormányzati célú felhasználásra csak az érintett személy kifejezett és egyértelmű beleegyezése esetén kerülhet sor.

Az európai modell központi elve az „kikényszeríthetőség". Az EU álláspontja szerint az adatok alanyait jogok illetik meg, amely jogokat kifejezett és egyértelmű jogi szabályozás keretei között kell megfogalmazni. Ezen kívül létezik egy olyan személy (adatvédelmi biztos) vagy szerv, akinek az a feladata, hogy a védelemre jogosult sze-

[2] Directive 97/66/EC on the processing of personal data and protection of privacy in the telecommunications sector (Rövien: Európai Telekommunikációs Irányelv).

[3] European Data Protection Directive.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (http://www.odpr.org/restofit/Legislation/Directive/Directive_Contents.html)

[5] Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997. (http://www2.echo.lu/legal/en/dataprot/protection.html)

mély nevében eljárjon, illetve a vonatkozó normáknak érvényt szerezzen. Ugyancsak elvárás az EU részéről, hogy azokban az országokban (3. állam), akikkel üzleti kapcsolatban állnak hasonló szintű védelemben részesüljenek a személyes adatok.

Az irányelv előírja a tagállamok számára, hogy azokat az adatokat is védelemben kell részesíteni, amelyeket másik – Európán kívüli – országba exportálják, illetve ott dolgozzák fel azokat. Az irányelv ezen cikkelyének hatására az EU-n kívüli államokban – amelyek továbbra is fenn szeretnék tartani a kapcsolatot az EU-s országokkal – is megindult a személyiségi jogok védelmét szolgáló jogi szabályozás kialakítása, illetve fejlesztése, mivel ennek hiányában megbénulhat az EU-val az információáramlás.

1.1. A 95/46/EK Irányelv rendelkezéseinek részletes bemutatása

Az Európai Parlament és a Tanács 1995. október 24-én fogadta el a 95/46/EK Irányelvet, amely „A személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról" rendelkezik.

A Közösségnek a Római Szerződésben (a továbbialban: RSz) megállapított, és az Európai Unióról szóló szerződés által módosított célkitűzései között szerepel a tagállamok közötti egyre szorosabb unió megteremtése, továbbá a Közösség gazdasági és társadalmi fejlődésének biztosítása, valamint az emberi jogok és alapvető szabadságjogok védelméről szóló európai egyezményben elismert alapvető jogok garantálása. Ennek értelmében nemzetiségtől és lakóhelytől függetlenül tiszteletben kell tartani a személyek alapvető jogait és szabadságjogait, különösen a magántitokhoz való jogukat, és hozzá kell járulniuk a gazdasági és társadalmi fejlődéshez, a kereskedelem kiterjedéséhez, valamint az egyének jólétéhez. Egy olyan belső piac kialakítása és működése, amelyben a RSz. 7a. cikkének megfelelően biztosított az áruk, a személyek, a szolgáltatások és a tőke szabad mozgása, nem csak azt kívánja meg, hogy a személyes adatok szabadon áramolhassanak egyik tagállamból a másikba, hanem azt is, hogy az egyének alapvető jogai biztosítottak legyenek. Megfigyelhető, hogy a Közösségben a gazdasági és társadalmi tevékenység számos területén egyre többször folyamodnak a személyes adatok kezeléséhez; mivel az informatika terén elért haladás az ilyen adatok kezelését és cseréjét lényegesen megkönnyíti;

A RSz. 7a. cikke értelmében a belső piac kialakításából és működéséből eredő gazdasági és társadalmi integráció szükségszerűen a személyes adatok határokon keresztüli áramlásának lényeges növekedéséhez vezetett – és ez a tendencia a jövőben még tovább fog erősödni – mindazok között, akik a tagállamokban magán- vagy állami szinten gazdasági vagy társadalmi tevékenységben vesznek részt. Mi az alapvető oka ennek a növekedésnek: *a)* a személyes adatok cseréje a különböző tagállamokban lévő vállalkozások között emelkedő tendenciát mutat; *b)* a különböző tagállamok nemzeti hatóságai a közösségi jog értelmében kötelesek olyan mértékben együttműködni és személyes adatokat cserélni, ami lehetővé teszi számukra feladataik ellátását, vagy a fellépést egy másik tagállam hatósága nevében a belső piac által képezett belső határok nélküli térség keretében és *c)* ezenfelül a növekvő tudományos és műszaki együttműködés és az új telekommunikációs hálózatok összehangolt bevezetése.

Ugyanakkor problémaként merül fel, hogy az egyes tagállamokban végzett személyesadat-kezelés terén az egyének jogai és szabadságjogai, különösen a magántitokhoz való jog védelmének szintjei közötti eltérések akadályozhatják az ilyen adatok egyik tagállamból a másikba történő továbbítását. Ebből eredően ezek az eltérések

akadályt jelentenek számos közösségi szintű gazdasági tevékenység elvégzésében, torzítják a versenyt, és hátráltatják a hatóságokat a közösségi jog szerinti feladataik teljesítésében. A védelmi szintek közötti ezen eltérések a nemzeti törvényi, rendeleti és közigazgatási rendelkezések sokféleségének tulajdoníthatók.

Fontos előfeltétel a személyes adatok áramlása előtti akadályok elhárítása érdekében, hogy az egyének jogai és szabadságjogai védelmének szintje az ilyen adatok kezelése terén minden tagállamban azonos legyen. Mivel ez a célkitűzés alapvető fontosságú az egységes belső piac megteremtése szempontjából, de a tagállamok ezt egyedül nem tudják megvalósítani – főként a tagállamok vonatkozó jogszabályai között jelenleg fennálló eltérések miatt –, ezért össze kell hangolni a tagállamok jogszabályait annak érdekében, hogy biztosított legyen a személyes adatok határokon keresztül történő áramlásának a RSz. 7a. cikkében meghatározott belső piac céljának megfelelő következetes szabályozása. Ezért szükséges az említett tagállami jogszabályok közelítését célzó közösségi fellépés.

Tagadhatatlan, hogy az egységesítés a fő vonal, de ezzel egyidejűleg létezik egy másik trend is. Ez utóbbin belül a tagállamok sok esetben az egyének jogai és szabadságjogai, különösen a magántitokhoz való jog védelmére hivatkozva igyekeznek akadályt gördíteni az adatvédelem harmonizációja elé. Sok tagállam megnyugvással vette tudomásul, hogy a Közösségi szintű szabályozás irányelv formájában történik, mivel ebből joggal lehet feltételezni, hogy a tagállamoknak marad annyi mozgástere, amelyet az irányelv végrehajtása során az üzleti és szociális partnerek céljaiknak megfelelően használhatnak. Ugyanakkor az irányelvvel történő szabályozás negatív hatása lehet, hogy az említett tagállami mozgástér keretein belül, és a közösségi joggal összhangban különbségek merülhetnek fel ezen irányelv végrehajtása során, ami negatív hatással lehet akár egy tagállamon belüli, akár a Közösségen belüli adatáramlásra.

A. Az irányelv célkitűzése

A személyes adatok kezelésére vonatkozó tagállami szintű jogszabályok célja az alapvető jogok és szabadságjogok, különösen a magántitokhoz való jog védelme. Ezt a premisszát mind az emberi jogok és alapvető szabadságjogok védelméről szóló európai egyezmény 8. cikke, mind a közösségi jog általános alapelvei elismerik. Ezért az említett belső jogszabályok közelítése nem vezethet az általuk nyújtott védelem szintjének csökkenéséhez, sőt, magas védelmi szintet kell biztosítson a Közösségen belül. Az EK Irányelve kiegészíti az Európa Tanács 1981. január 28-i, az egyéneknek a személyes adataik gépi feldolgozása során való védelméről szóló egyezményében foglaltakat.

B. Az irányelv tárgyi hatálya

Az irányelvet az olyan személyes adatok részben vagy egészben automatizált eszközök által, illetve nem elektronikus eszközökkel történő kezelésére nézve kell alkalmazni, amelyek valamely nyilvántartási rendszer részét képezik, vagy azokat egy nyilvántartási rendszer részének szánják. Az irányelv értelmében az egyének védelme tehát a gépi adatkezelésre éppúgy vonatkozik, mint a kézi adatkezelésre. A személyiségi jogok védelme nem függhet az alkalmazott módszertől, mivel ez a jog megkerüléshez vezethetne. Ugyanakkor az irányelv a kézi adatkezelés tekintetében csak a nyilvántartási rendszerre terjed ki, a nem rendszerezett iratokra nem.

Az irányelv tárgyi hatálya nem terjed ki az alábbi személyesadat-kezelésekre:

a) a közösségi jog hatályán kívül eső tevékenységek (pl. az Európai Unióról szóló Szerződés V. és VI. címei),
b) a közbiztonságra, a védelemre, az állambiztonságra (beleértve az ország gazdasági jólétét is, ha az feldolgozási művelet állambiztonsági ügyre vonatkozik),
c) a büntetőjog területén az állami tevékenységekkel kapcsolatos feldolgozási műveletek,
d) a természetes személy által tisztán magáncélból, vagy otthoni tevékenység keretében végzett adatfeldolgozás.

Ugyancsak kizárt az Irányelv tárgyi hatálya alól a természetes személyek által végzett adatkezelés, amennyiben azt kizárólag személyes vagy házi használatra, például levelezés, vagy címjegyzékek vezetése során végzik.

A jogi személyek védelmére vonatkozó jogalkotás nem tartozik az EK irányelv hatálya alá.

Az újságírás, az irodalmi, vagy művészi kifejezés céljából végzett hang-, vagy képadatok kezelését tekintve, különösen audiovizuális téren az irányelv alapelveit korlátozott módon kell alkalmazni (lásd 9. Cikkely).

Annak biztosítása érdekében, hogy az egyéneket ne lehessen megfosztani attól a védelemtől, amelyre az irányelv értelmében jogosultak, a Közösség területén végzett minden személyesadat-kezelési tevékenységet a tagállamok valamelyikének jogszabályai szerint kell végrehajtani. Következésképpen, a valamely tagállamban letelepedett adatkezelő felelőssége mellett végzett adatkezelésre ennek a tagállamnak a jogszabályai vonatkoznak. A valamely tagállamban való letelepedés magában foglalja a tevékenység tartós jellegű, tényleges gyakorlását. A letelepedés jogi formája – legyen akár egyszerűen fióktelep, akár jogi személyiséggel rendelkező leányvállalat – e tekintetben nem meghatározó tényező. Előfordul, hogy egy adatkezelő akár több tagállamban is letelepedett, főként leányvállalatok révén. Ilyenkor, a nemzeti szabályozás megkerülésének kizárása érdekében gondoskodnia kell arról, hogy minden egyes létesítménye megfeleljen a tevékenységére alkalmazandó nemzeti jogszabályok által meghatározott kötelezettségeknek.

Az is előfordul, hogy az adatkezelést valamely harmadik országban letelepedett személy végzi. Ez a tény önmagában nem gátolhatja az egyéneknek az Irányelvben elrendelt védelmét. Ilyen esetekben az adatkezelésre annak a tagállamnak a jogszabályai irányadók, amelyben az alkalmazott eszközök találhatók, továbbá garanciákat kell találni arra, hogy EK Irányelvben meghatározott jogok és kötelezettségek a gyakorlatban is érvényesüljenek.

A tagállamok az egyének védelmének megvalósításáról gondoskodhatnak *a)* általános jogszabály keretében, vagy *b)* ágazati jogszabályokban (mint például a statisztikai intézetekre vonatkozó szabályozás).

C. Az irányelv alapelvei

Az irányelv csak alapvető elveket határoz meg – elsősorban az adatminőségre és az adatkezelésre vonatkozó elvek formájában – és ezek keretein belül minden tagállam

saját hatáskörében dolgozza ki, hogy a személyes adatok kezelése milyen feltételek mellett jogszerű.

A védelem elveit minden azonosított vagy azonosítható személyre vonatkozó információ esetében alkalmazni kell. Annak meghatározására, hogy egy személy azonosítható-e, minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására. A védelem elvei nem alkalmazhatók az olyan módon anonimmá tett adatokra, ahol az érintett a továbbiakban nem azonosítható.

1. Az alkalmazandó nemzeti jog elve

A személyes adatok kezelésére minden tagállam az irányelvnek megfelelően elfogadott nemzeti rendelkezéseket alkalmazza.

2. Az adatok minőségére vonatkozó elvek:

a) Tisztességes és törvényes adatkezelés;
b) Csak meghatározott, egyértelmű és törvényes célból lehet adatgyűjtést folytatni, és az adatok további kezelése sem végezhető e célokkal összeférhetetlen módon;[6]
c) Összegyűjtésük és/vagy további kezelésük célja szempontjából megfelelőnek, relevánsnak és nem túlzott mértékűnek kell lenniük;
d) Pontosnak, és ha szükséges, időszerűnek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy a pontatlan vagy hiányos adatok, tekintettel összegyűjtésük vagy további kezelésük céljaira, törlésre vagy kiigazításra kerüljenek;
e) Tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok összegyűjtése vagy további kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.[7]

Ezek az alapelvek kísértetiesen hasonlítanak az OECD által alkotott alapelvekhez.

3. Az adatkezelés jogszerűvé tételére vonatkozó kritériumok

A személyes adatok csak abban az esetben kezelhetőek, ha: *a)* az érintett ahhoz egyértelmű hozzájárulását adta; vagy *b)* az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges; vagy *c)* az adatkezelés az adatkezelőre vonatkozó jogi kötelezettségnek való megfeleléshez szükséges; vagy *d)* kezelésük az érintett alapvető érdekei védelméhez szükséges; vagy *e)* az adatkezelés közérdekből elvégzendő feladat végrehajtásához vagy az adatkezelőre, illetve az adatokról tudomást szerző harmadik félre ruházott hivatali hatáskör gyakorlásához szükséges, vagy *f)* a feldolgozásra az adatkezelő, vagy az adatokról tudomást szerző harmadik fél,

[6] A személyes adatok további kezelése történelmi, statisztikai vagy tudományos célokra nem tekintendő összeférhetetlennek, amennyiben a tagállamok biztosítják a megfelelő garanciákat.

[7] A tagállamok állapítják meg a személyes adatok történelmi, statisztikai vagy tudományos célból, hosszabb ideig történő tárolásának megfelelő garanciáit.

vagy felek által felmutatott jogszerű érdekek szempontjából van szükség, kivéve, ha ezeknél az érdekeknél magasabb rendűek az egyén alapvető szabadságjogai.

Különleges (érzékeny) adatkategóriák kezelése: Az irányelv értelmében a tagállamok szabályozása megtilthatja az olyan személyes adatok kezelését, amelyek betekintést engednek a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy filozófiai meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkozó kérdésekbe. Nem lehet alkalmazni ezt a megszorítást abban az esetben, ha: *a)* az érintett kifejezett hozzájárulását adta az említett adatok kezeléséhez, kivéve, ha a közösségi intézmény vagy szerv belső szabályai eltérően rendelkeznek; *b)* az adatkezelés az adatkezelő bizonyos jogai és kötelezettségei betartása érdekében szükséges a foglalkoztatási jogszabályok területén, amennyiben a megfelelő biztosítékokról rendelkező nemzeti jogszabályok ezt lehetővé teszik, illetve *c)* az adatkezelés az érintett vagy más személy alapvető érdekeinek védelméhez szükséges abban az esetben, ha az érintett fizikailag vagy jogilag képtelen a hozzájárulását adni, illetve *d)* az adatkezelés valamely alapítvány, egyesület vagy non-profit szervezet megfelelő biztosítékok mellett végzett törvényes tevékenysége keretében történik, politikai, filozófiai, vallási vagy szakszervezeti céllal, azzal a feltétellel, hogy a kezelés kizárólag az ilyen szerv tagjaira, vagy olyan személyekre vonatkozik, akik azzal rendszeres kapcsolatban állnak a szerv céljainak megfelelően, és az adatok nem adhatók ki harmadik fél részére az érintettek hozzájárulása nélkül, illetve *e)* az adatkezelés olyan adatokra vonatkozik, amelyeket az érintett köztudottan nyilvánosságra hozott, vagy amelyek jogi követelések megállapításához, gyakorlásához vagy védelméhez szükségesek.

Nem tiltható meg a személyes adatok kezelése akkor sem, ha az adatok kezelése megelőzési célú gyógyszer, orvosi diagnózis, gondozás vagy kezelés alkalmazása vagy egészségügyi szolgáltatások igazgatása céljából szükséges, és ha az adatokat szakmai titoktartási kötelezettség alá eső egészségügyi szakember vagy azzal egyenértékű titoktartási kötelezettség alá eső más személy kezeli.

A tagállamok határozzák meg a nemzeti azonosító számok és egyéb általános jellegű azonosító jelek kezelésének feltételeit.

4. A tájékoztatáshoz való jog

Az adatkezelőnek vagy képviselőjének legalább az alábbiakról kell tájékoztatnia az érintettet, akitől a rá vonatkozó adatokat gyűjtik, kivéve, ha az érintett már rendelkezik ezen információkkal:

a) az adatkezelő, vagy ha van ilyen, képviselőjének személye;
b) az adatkezelés célja, amelyre az adatokat szánják;
c) minden olyan további adatot, mint például:

- az adatok címzettjei, illetve a címzettek kategóriái,
- a kérdések megválaszolása kötelező-e vagy önkéntes, továbbá a válaszadás elmulasztásának lehetséges következményei,
- betekintési jog és az érintettre vonatkozó adatok kiigazításához való jog, amennyiben e további információk, tekintettel az adatgyűjtés sajátos körülményeire, az érintett vonatkozásában a tisztességes adatkezelés biztosításához szükségesek.

Abban az esetben, ha az adatokat nem az érintettől szerezték be, a tagállamoknak rendelkezniük kell arról, hogy az adatkezelő vagy képviselője a személyes adatok felvételének elvállalásakor, illetve, ha az adatokat harmadik személyhez szándékoznak továbbítani, legkésőbb az adatok első nyilvánosságra hozatalakor köteles az érintettel legalább az alábbi információkat közölni, kivéve, ha az érintett már rendelkezik ezekkel az információkkal:

a) az adatkezelő, vagy ha van ilyen, képviselőjének személye;
b) az adatkezelés célja;
c) bármely egyéb információ, mint például:

- az érintett adatok kategóriái,
- az adatok címzettjei vagy a címzettek kategóriái,
- betekintési jog és az érintettre vonatkozó adatok kiigazításához való jog, amennyiben e további információk, tekintettel az adatgyűjtés sajátos körülményeire, az érintett vonatkozásában a tisztességes adatkezelés biztosításához szükségesek.

A fenti rendelkezés nem alkalmazható, különösen a statisztikai célú vagy történelmi, vagy tudományos célú adatkezelés esetében, ha a kérdéses információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel, illetve ha a nyilvántartást vagy a nyilvánosságra hozatalt jogszabály kifejezetten előírja. Ezekben az esetekben a tagállamoknak garantálniuk kell a megfelelő biztosítékokat.

5. Az adatkezelés titkossága

Bármely, az adatkezelő vagy az adatfeldolgozó meghatalmazásával eljáró személy, beleértve magát az adatfeldolgozót is, aki a személyes adatokhoz hozzáféréssel rendelkezik, kizárólag az adatkezelő utasítása alapján kezelheti ezeket az adatokat, kivéve, ha erre őt jogszabály kötelezi.

6. Az adatkezelés biztonsága

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő műszaki és szervezeti intézkedéseket a személyes adatok véletlen vagy jogszerűtlen megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében, különösen, ha a kezelés közben az adatokat hálózaton keresztül továbbítják, továbbá a feldolgozás minden más jogellenes formája ellen.

Tekintettel a technika vívmányaira és alkalmazásuk költségeire, ezen intézkedéseknek olyan szintű biztonságot kell nyújtaniuk, amely megfelel az adatkezelés által jelentett kockázatoknak és a védendő adatok jellegének.

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő – amennyiben az adatkezelés az ő nevében történik – köteles olyan adatfeldolgozót választani, aki a műszaki biztonsági intézkedések és az elvégzendő adatkezelésre vonatkozó szervezeti intézkedések tekintetében megfelelő garanciákat nyújt, továbbá köteles biztosítani az említett intézkedések teljesítését.

D. A felügyeleti hatóság értesítésére vonatkozó kötelezettség

A tagállamoknak rendelkezniük kell arról, hogy az adatkezelő vagy annak képviselője, ha van ilyen, értesítse a tagállam felügyeleti hatóságot akár egyetlen, akár több, összefüggő célt szolgáló, részben vagy egészen gépi úton történő adatkezelési művelet vagy műveletsorozat elvégzését megelőzően.

A tagállamok rendelkezhetnek arról, hogy az értesítési kötelezettség ne vonatkozzon arra az adatkezelésre, amelynek kizárólagos célja egy olyan nyilvántartás vezetése, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll.

E. Mentességek és korlátozások

A tagállamok jogi intézkedéseket fogadhatnak el az adatok minőségére [6. cikk (1) bek.], az érintett tájékoztatására (10. cikk), a más személytől beszerzett adatokról történő tájékoztatásra [11. cikk (1) bek.], valamint az adatkezelési műveletek nyilvánosságának biztosítására (21. Cikk) vonatkozó jogok és kötelezettségek körének korlátozására, amennyiben a korlátozás az alábbiak biztosításához szükséges: *a)* nemzetbiztonság; *b)* honvédelem; *c)* közbiztonság; *d)* bűncselekmények vagy a kérdéses foglalkozások szakmai etikai normáinak a megsértésének megelőzése, a jogszabálysértések kiderítésére irányuló nyomozása és az ezekkel kapcsolatos eljárások lefolytatása, *e)* valamely tagállam vagy az Európai Unió fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket; *f)* a c), d) és e) pontban említett esetekben esetlegesen a közhatalom gyakorlásához kapcsolódó ellenőrzési, felügyeleti és szabályozási tevékenység és *g)* az érintett, vagy mások jogainak és szabadságjogainak védelme.

F. Az érintett kifogásolási joga

A tagállamoknak biztosítaniuk kell az érintettnek, hogy *a)* sajátos helyzetével kapcsolatos lényeges jogos érdekből bármikor kifogást emelhessen a rá vonatkozó adatok kezelése ellen. Jogos kifogás esetén az adatkezelő által kezdeményezett adatkezelés a továbbiakban nem terjedhet ki a szóban forgó adatokra és *b)* kérelemre és térítésmentesen kifogást emelhessen az olyan, rá vonatkozó személyes adatok kezelése ellen, amelyekkel kapcsolatban az adatkezelő előre jelzi, hogy feldolgozásuk célja direkt-marketing, illetve hogy tájékoztassák személyes adatainak harmadik személyeknek első alkalommal történő tudomására hozása, vagy a nevükben direkt marketing céljára történő felhasználás előtt. Az érintett szervek számára az ilyen nyilvánosságra hozatal vagy felhasználás elleni kifogás jogát kifejezetten biztosítani kell.

G. Automatizált egyéni döntések

Az irányelv értelmében a tagállamok kötelessége, hogy minden személynek biztosítsa a jogot arra, hogy ne terjedhessen ki rájuk olyan határozat hatálya, amely rájuk nézve jogi hatással járna, vagy őket jelentős mértékben érintené, és amelynek alapja kizárólag gépi adatkezelés, amelynek célja a rá vonatkozó egyes olyan személyes szempontok kiértéke-

lése, mint például a munkahelyi teljesítmény, a hitelképesség, a megbízhatóság, az életvitel stb.

Ugyanakkor a tagállamok úgy is rendelkezhetnek, hogy a fentebb említett határozat hatálya kiterjedhet a személyre, amennyiben a határozatot:

a) valamely szerződés megkötése vagy teljesítése során hozták, feltéve, hogy az érintett által a szerződés megkötése vagy teljesítése iránt benyújtott kérelmet teljesítették, vagy jogos érdekének biztosítására megfelelő biztosítékok állnak rendelkezésre, mint például a véleményének kinyilvánítását lehetővé tevő intézkedések; vagy
b) olyan jogszabály teszi lehetővé, amely az érintett jogos érdekeit biztosító intézkedéseket is megállapítja.

H. Felelősség

Mindenki, aki törvénytelen adatkezelési művelet vagy az adatvédelmi irányelv értelmében elfogadott nemzeti rendelkezésekkel összeegyeztethetetlen intézkedés eredményeképpen kárt szenvedett, az adatkezelőtől kártérítésre jogosult az elszenvedett károkért. Az adatkezelő részben vagy egészben mentesül e felelősség alól, ha bizonyítja, hogy a kárt okozó eseményért nem felelős.

I. A személyes adatok harmadik országokba irányuló továbbítása

A tagállamoknak rendelkezniük kell arról, hogy a feldolgozásra kerülő vagy továbbítás után feldolgozásra szánt személyes adatok csak akkor továbbíthatók harmadik országba, ha az ezen irányelv egyéb rendelkezései értelmében elfogadott nemzeti rendelkezéseknek való megfelelés sérelme nélkül az adott harmadik ország megfelelő védelmi szintet tud biztosítani.

A fenti tilalomtól eltérően, és amennyiben az adott esetre vonatkozó belföldi jogszabályok másképp nem rendelkeznek, a tagállamok rendelkeznek arról, hogy a személyes adatok olyan harmadik országba irányuló továbbítása vagy továbbítás-sorozata, amely nem biztosít megfelelő szintű védelmet, csak a következő feltételek mellett történhessen:

a) az érintett egyértelműen hozzájárulását adta a tervezett továbbításhoz; vagy
b) a továbbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérelmére hozott, szerződést megelőző intézkedések végrehajtásához szükséges; vagy
c) a továbbítás az adatkezelő és valamely harmadik fél közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges; vagy
d) a továbbítás fontos közérdekből vagy jogi követelések létrejötte, érvényesítése vagy védelme miatt szükséges, illetve azt jogszabály írja elő; vagy
e) a továbbítás az érintett alapvető érdekeinek védelme miatt szükséges; vagy
f) a továbbítást olyan nyilvántartásból végzik, amely a törvények vagy rendeletek értelmében a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság, vagy bármely jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll, amennyiben a jogszabályok által a betekintésre megállapított feltételek az adott esetben teljesülnek.

J. Az adatvédelem intézményrendszere

1. A tagállamokban működő felügyeleti hatóság

Minden tagállamnak létre kell hoznia egy felügyeleti hatóságot. Ennek a feladata az adatvédelmi irányelvből a tagállam által elfogadott nemzeti rendelkezéseknek a saját területén történő alkalmazásának az ellenőrzése. E hatóságok a rájuk ruházott feladatok gyakorlásában teljes függetlenségben járnak el.

A hatóságok különösen a következő jogosultságokkal rendelkeznek:

a) nyomozati jog (pl. az adatkezelési műveletek tárgyát képező adatokhoz való hozzáférés joga, továbbá a felügyeleti feladatok ellátásához szükséges adatok gyűjtésének joga),
b) tényleges beavatkozási jogosultság (pl. az adatok zárolásának, törlésének vagy megsemmisítésének elrendelése, az adatkezelés átmeneti vagy végleges tilalmának megállapítása, az adatkezelő figyelmeztetése vagy megrovása, illetve az ügy nemzeti parlament vagy más politikai intézmény elé terjesztése stb).
c) bírósági eljárásban való részvétel joga (az irányelv értelmében elfogadott nemzeti rendelkezések megsértése esetén, továbbá e jogsértések igazságügyi szervek elé terjesztésének joga).

A felügyeleti hatóság kifogásolható határozatai bíróság előtt megtámadhatók.

A felügyeleti hatóságok foglalkoznak a személyes adatok kezelése vonatkozásában az egyének jogainak, illetve szabadságjogainak védelmével kapcsolatos, bármely személy vagy az őt képviselő szervezet által benyújtott kérelmekkel. A kérelem elbírálásáról az érintett személyt értesíteni kell.

A felügyeleti hatóságoknak foglalkozniuk kell különösen az adatkezelés törvényességének ellenőrzésére irányuló, bármely személy által benyújtott kérelemmel, amennyiben az ezen irányelv 13. cikkének értelmében elfogadott nemzeti rendelkezések alkalmazhatóak. Az érintett személyt mindenképpen értesíteni kell, ha az ellenőrzés megtörtént.

2. A személyes adatkezelés vonatkozásában az egyének védelmével foglalkozó munkacsoport

Az adatvédelem intézményrendszerének egy másik megjelenési formája az egyének védelmével foglalkozó munkacsoport. A munkacsoport tanácsadói státuszban működik és függetlenül jár el. A munkacsoport az egyes tagállamok által kijelölt felügyeleti hatóság vagy hatóságok képviselőjéből, a közösségi intézmények és szervek nevében létrehozott hatóság vagy hatóságok képviselőjéből, továbbá a Bizottság egy képviselőjéből áll. A munkacsoport minden egyes tagját az az intézmény, hatóság, vagy hatóságok jelöli vagy jelölik ki, amelyet, illetve amelyeket képvisel. Ha a tagállam több felügyeleti hatóságot jelöl ki, ezek közös képviselőt állítanak. Ugyanez vonatkozik a közösségi intézmények és szervek nevében létrehozott hatóságokra is.

A munkacsoport hatásköre:

a) megvizsgál minden, az irányelv értelmében elfogadott nemzeti intézkedések alkalmazási körébe tartozó kérdést, azok egységes alkalmazása érdekében;

b) véleményt nyilvánít a Bizottságnak a Közösség és a harmadik országok védelmének szintjéről;
c) tanácsot ad a Bizottságnak az adatvédelmi irányelv javasolt módosításaira;
d) véleményt nyilvánít a közösségi szinten kidolgozott eljárási szabályzatokról.

A munkacsoport saját kezdeményezésére ajánlásokat tehet bármely kérdésben, amely a személyes adatok közösségen belüli kezelése tekintetében a személyek védelmével kapcsolatos. A munkacsoport véleményeit és ajánlásait továbbítani kell a Bizottsághoz, valamint a 31. cikkben említett bizottsághoz.

3. A Közösségi szintű intézményi védelem: A bizottság

A Bizottságot a tagállamok képviselőiből álló bizottság segíti, amelynek elnöke a Bizottság képviselője. A Bizottság képviselője tervezetet nyújt be a bizottságnak a meghozandó intézkedésekről. A bizottság véleményt nyilvánít a tervezetről az elnök által az ügy sürgősségének megfelelően megállapított határidőn belül.

1.2. A személyes adat védelemről rendelkező 95/46/EC irányelvének gyakorlati vonatkozásai

A személyes adatok védelmére vonatkozó jogi szabályozás számos vonatkozásban érinti a munkavállalók ellenőrzését és megfigyelését. Attól a perctől kezdve, hogy a személyes adatok megszerzésre és feldolgozásra kerülnek a személyes adatok védelmét szolgáló jogszabályokat – beleértve az EU-s irányelvet is – alkalmazni kell. Az irányelv rendelkezéseinek a végrehajtása nem minden esetben egyértelmű. Például, a manuális adatfeldolgozás (manual processing of personal data) kérdése; vagy az irányelv 2 (c) cikkelye értelmében rendszerezett adatállománynak (structured set of data) teinthető-e a titkár/nő asztalán heverő írásban benyújtott pályázat; vagy ahhoz, hogy személyes adatgyűjtő rendszerről (personal data filing system) beszéljünk szükség van-e több személy adataira. Ugyancsak jogalkalmazási problémát vet fel a személyes adatok védelmére vonatkozó 96/46/EGK irányelv és a telekommunikációs szektorban a személyiségi jogok védelmét szabályozó 97/66/EGK irányelv kapcsolata. Jelenleg ez a kérdés az EU szintjén sem került kellőképpen tárgyalásra.[8]

Az Európai Unió Adatvédelemmel foglalkozó biztosa (Data Protection Comissioner) az információs technológia és telekommunikáció munkahelyi alkalmazásából eredő problémák kiküszöbölése érdekében számos ajánlást fogalmazott meg. Ezek a problémák túlnyomó többségében a munkahelyeken a munkavállalóra vonatkozó adatok védelmére vonatkoznak. A munkaviszony létesítése és fennállása során – kölcsönösen - számos információ jut a szerződő felek tudomására. Ezen információk védelméhez mindkét félnek nyomós indoka fűződik. A közelmúltban bekövetkező robbanásszerű információs robbanás megsokszorozta a lehetőségét és a ténylegesen összegyűjtött adatok számát. Leegyszerűsödtek az eljárások, az adatfeldolgozás gyorsabbá vált. Ugyanakkor ezt a felgyorsult folyamatot nem követte ugyanilyen sebességgel a munkavállalók adatainak, illetve az ehhez kapcsolódó személyiségi jogoknak a védelme.

[8] Erre a megállapításra egy 2001. október 4–5 között, Frank professzor elnökletével lezajlott jogi szakértokbol álló kerekasztal konferencia résztvevoi jutottak.

Ugyanakkor kialakult néhány új gyakorlat. Lehetséges a munkavállalók tevékenységének – különböző szempontok és célok szerinti – folyamatos megfigyelése és a róluk történő adatok gyűjtése, még akkor is, ha erről ők nem is tudnak. Az ilyen jellegű megfigyelések gyakorlata egyre szélesebb körben terjed és – bizonyos megszorítások között – egyre inkább elfogadottá válik. Milyen indokok állnak ennek a hátterében: *a)* az ilyen jellegű megfigyeléseket elsősorban a munkavállalók biztonsága indokolja, továbbá *b)* a megfigyelések tapasztalatainak elemzése után a munkavégzés hatékonyságát és ennek eredményeként a termelékenységet (ergonómiai szempontok) lehet növelni, *c)* hatalmas információbázis gyűjthető a munkavállalók viselkedéséről, személyiségéről és tevékenységéről.

Ezzel a pozitív megközelítéssel szemben a munkavállalókról összegyűjtött és a munkáltató vagy esetleg külső harmadik személy számára rendelkezésre álló hatalmas információmennyiség sebezhetővé teszi a munkavállalót és sértheti a személyiségi jogait. Ezért van szükség a személyes adatok jogi védelmére.

Felmerülhet a kérdés, hogy mit értünk munkahely alatt. A vonatkozó EU-s megközelítés értelmében a munkahelyet kiterjesztően kell értelmezni: minden olyan lehetséges hely munkahelynek minősül, ahol a munkavállaló – munkáltatói utasításra – a munkavégzési tevékenységét folytatja. Ez lehet a munkáltató telephelye, a munkavállaló gépkocsija vagy esetleg a saját lakása (kiváló példa lehet erre az egyre jobban terjedő telemunka típusú munkavégzés).

A munkavállalók személyiségi jogainak védelmét szolgáló jogi normák alulreprezentáltak az egyes országok munkajogi szabályozásában. Ezért fontos szerephez jutnak a nemzetközi és az EU-s normák. Ezek segítik a jogalkotókat, de egyidejűleg segítenek a munkáltatóknak is abban, hogy kialakuljon egy kultúrált munkavégzési környezet, amelyben nem sérülnek a munkavállalók személyiségi jogai.

1.2.1. A 95/46/EC Irányelv alapján történő e-mail/Internet megfigyelésnél alkalmazott általános elvek

A következő adatvédelmi elveket a 95/46/EC irányelv tartalmazza. A gyakorlatban végzett munkáltatói megfigyeléseknek és ellenőrzéseknek ezekkel az elvekkel összhangban kell állniuk.

a) Szükségesség (necessity)

Mielőtt bármilyen elektronikus megfigyelést kezdeményezne a munkáltató kötelessége annak az eldöntése, hogy az ilyen típusú megfigyelésre abszolút értelemben szükség van-e vagy sem. A döntés meghozatala előtt alapvetően azt kell mérlegelni, hogy a munkavállaló teljesítményének ellenőrzésére szolgáló hagyományos eszközökkel és módszerekkel – amelyek kevésbé veszélyeztetik a munkavállaló személyiségi jogait – az elérendő cél megvalósítható-e. A munkavállaló e-mail/Internet forgalmának a megfigyelése csak kivételes esetben lehet szükséges. Például a munkavállaló valamilyen bűncselekményt követ el és ennek az elektronikus megfigyelés segítségével történő megelőzése vagy a munkavállalói szándék kifürkészése a munkáltató közvetlen gazdasági érdeke, mivel ilyen esetben is kártérítési felelősség terhelheti a munkáltatót. Ugyancsak jó példa, ha a munkáltató az elektronikus rendszer működésének biztonsága érdekében – vírusfertőzés megelőzése stb. – figyeli a munkahelyi rendszert.

Azt is meg kell jegyezni, hogy bizonyos esetekben a munkavállaló levelezésének a megtekintése szükségszerű és indokolt. Gondoljunk arra az esetre, amikor a munkavállaló szabadság vagy betegség miatt hosszabb időre távol van a munkahelyétől. A munkáltató gazdasági érdeke azt diktálja, hogy ilyenkor a munkavállalót helyettesítő munkatárs be tudjon lépni a rendszerbe. Ez nem tekinthető illegálisnak. Mindkét esetben feltétel, hogy a szükségesség és a jogszerűség határain belül maradjon a megfigyelést végző személy.

A „szükségesség" alapelvének van egy másik vetülete is. Ennek értelmében a munkáltató az összegyűjtött adatokat csak addig tárolhatja, amíg az eredeti cél megvalósítása érdekében szükséges. Azt követően haladéktalanul törölni kell a rendszerből.

b) Célhozkötöttség elve (finality)

A célhozkötöttség elve azt jelenti, hogy az adatokat egy konkrétan meghatározott és jogszerű célból gyűjtik össze és az eredeti célkitűzéstől eltérő mindennemű további feldolgozás és kezelés tilos. Például, ha egy adatot a kommunikációs rendszer vírusmenetességének az ellenőrzésére gyűjtöttek, akkor az így nyert adatot nem lehet továbbadni például a munkavállaló teljesítményének az értékelésére. A tilalom indoka, hogy eredetileg nem ez volt az adatgyűjtés célja.

c) Áttekinthetőség (transparency)

Az alapelv eredeti jelentése, hogy a munkáltatói magatartásnak világosnak és nyitottnak kell lennie. Ennek értelmében a munkáltató fő szabályként titkos e-mail megfigyelést nem végezhet. Ez alól kivételt csak az Irányelv 13. Cikkelyében kapott felhatalmazás alapján megalkotott tagállami szabályozás adhat. Ilyen kivételes ok lehet a nemzetbiztonsági vagy közbiztonsági ok, nyomozás, az adatalany vagy más személy szabadságjogainak a védelme. Az áttekinthetőség alapelvét további két részre lehet bontani.

ca) Az adatalany megfelelő információkkal való ellátása

A munkáltatónak kötelessége, hogy világos és pontos információval lássa el a munkavállalóját a munkáltatónál alkalmazott e-mail/Internet megfigyelésre vonatkozó szabályokról. A munkavállalót informálni kell arról, hogy milyen speciális feltételek esetén kerülhet sor a megfigyelésre, tájékoztatni kell a megfigyelés terjedelméről (mire terjed ki a megfigyelés). A munkavállalót alapvetően az alábbi kérdésekről kell tájékoztatni:

– A munkáltató elektronikus eszközei közül melyiket használhatja saját célra (magánjellegű kommunikációra). Ilyen esetben közölni kell az esetleges megszorításokat is: mennyi ideig, mely napszakban használhatja stb.

– A megfigyelés okáról és céljáról. Amennyiben a munkáltató megengedte a munkahelyi kommunikációs infrastruktúra magáncélú használatát, akkor is csak különösen indokolt esetben ellenőrizheti a munkavállaló magáncélú levelezését. A fő szabály tehát az, hogy annak ellenére, hogy a munkavállaló a munkahelyi gépen, esetleg munkaidőben használja magáncélú levelezésre a rendszert, a munkáltató ekkor sem nézhet bele a levelezésébe, csak nagyon kivételes esetben. Ilyen kivételes eset, amikor például az információs rendszer biztonságának megőrzése érdekében – pl. víruskeresés – kell ellenőrizni a magánlevelezést. Megjegyezzük, hogy a munkáltató joga ilyen esetben sem

terjed ki arra, hogy a munkavállaló magáncélú levelezésének tartalmát megtekintse, hanem csak a technikai szempontból szükséges ellenőrzés az engedélyezett. Konkrétan egy vírusellenőrzés során megnyithatja a munkavállaló privát levelezési címét, de csak azt nézheti meg, hogy valamelyik file vagy adatállomány fertőzött-e vagy sem. Nagyon fontos kihangsúlyozni, hogy nem olvashat bele a magánlevelekbe, nem töltheti le azokat, stb.

– A munkavállalót a megfigyelés részleteiről is tájékoztatni kell: ki, mit, mikor, hogyan fog ellenőrizni vagy megfigyelni.

– Részletes végrehajtás szabályok megalkotása, amelyek meghatározzák, hogy a munkavállalót hogyan és mikor kell értesíteni, ha a munkáltatói belső kommunikációs szabályzatot megsérti. Lehetőséget kell számára biztosítani, hogy az ellene felhozott vádakra reagálhasson.

Praktikus szempontból kívánatos, hogy a munkáltató azonnal értesítse a munkavállalót, ha a belső kommunikációs szabályzat megsértését észleli. Kivételt képez, ha a munkavállaló megfigyelése indokolt. A gyors értesítés nem okozhat problémát, hiszen számos olyan program létezik, amelyen keresztül a munkáltató azonnal tudja informálni a munkavállalót. Ezzel a módszerrel számos későbbi félreértést lehet szinte azonnal megelőzni.

Egy további példa az „áttekinthetőség" elvének az érvényesülésére az a gyakorlat, amikor a munkahelyi belső kommunikációs szabályzat elfogadása előtt a munkáltató informálja a szociális partnereket vagy konzultál velük. Ezzel összefüggésben ki kell hangsúlyozni, hogy a munkavállalók elektronikus kommunikációjának a megfigyelése és az ellenőrzés elrendelése a 2002/14/EC irányelv hatálya alá tartozik. Az irányelv a munkavállalókkal történő konzultációt és információáramlást teszi kötelezővé olyan esetekben, amikor a döntés alapvető változást eredményezhet a munkaszervezetben vagy a felek szerződéses viszonyában. Tagállami szabályozás vagy kollektív szerződés a munkavállalóra nézve még ennél is kedvezőbb szabályt tartalmazhat. A kollektív szerződések nem pusztán arra kötelezik a munkáltatót, hogy informálja vagy konzultáljon a munkavállalói érdekképviselettel a megfigyelési, illetve ellenőrzési rendszer bevezetése előtt, hanem még a döntés meghozatala előtti konzultációt ír elő számára.

A kollektív szerződések ugyancsak rendelkezhetnek a munkavállaló megengedett munkahelyi e-mail/Internet használatának feltételeiről. Beleértve a munkáltató ellenőrzési és megfigyelési jogának a terjedelmét is.

cb) A Felügyeleti Szerv értesítési kötelezettsége az automatikus vagy részben automatikus megfigyelési rendszer bevezetése előtt

Ez a munkáltatói kötelezettség az *„áttekinthetőségi alapelv"* érvényesülésének egy másik vetülete. Ennek keretében biztosított az adatalany számára, hogy az Adatvédelmi Nyilvántartásban (Data Protection register) megnézhesse, hogy milyen jellegű adatokat gyűjtenek, milyen célból teszik azt, kinek a részére gyűjtik az adatot stb.[9]

[9] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 16.

d) Hozzáférhetőség (Right of access)

A 95/46/EC irányelv értelmében adatalanynak – függetlenül attól hogy munkavállalóról vagy bármely más természetes személyről van szó – joga van ahhoz, hogy a róla gyűjtött adatokat megtekinthesse. Ha azt észleli, hogy azok valamilyen okból kifolyólag hibásak – nem felel meg az EU-s irányelv előírásainak –, akkor azok kijavítását vagy törlését kérheti vagy megakadályozhatja a további feldolgozásukat. A munkavállalókat ez a jog korlátozás nélkül megilleti. Természetesen ezt a jogot csak egy meghatározott normális időintervallumon belül és nem indokolatlan költség árán gyakorolhatják. A munkavállalók ezen joga egy hatékony fegyver, amely segítségével nagy valószínűséggel ki tudják kényszeríteni a munkáltatók jogszerű és korrekt megfigyelési és adatgyűjtési magatartását. Ez a megoldás néhány speciális adatbázis esetén – például a munkavállalói értékeléssel kapcsolatos adatok stb. – okozhat csak problémát. Erre vonatkozóan született az 1/2000 Ajánlás, amely a munkavállalói értékeléssel kapcsolatos adatokra vonatkozó speciális eljárási kérdésekről szól.

e) Jogszerűség (legitimacy)

Az alapelv azt jelenti, hogy az adatgyűjtés és feldolgozás csak jogilag engedélyezett célból történhet. A jogszerűség tekintetében iránymutatást az Irányelv 7. Cikkelye és a tagállami belső szabályozás ad. Az irányelv 7 (f) cikkelye kimondja, hogy az irányelv értelmében a munkavállaló személyes adatát csak akkor lehet kezelni, ha azt a munkáltatónak jogos érdeke indokolja, de ilyenkor is maximálisan ügyelni kell arra, hogy a munkavállalók alapvető emberi jogai ne sérüljenek. A munkáltató jogos érdeke lehet annak a megakadályozása, hogy a munkavállaló bizalmas információkat vagy know-how-t átadja a versenytárs munkáltatónak.

Az ún. érzékeny adatok kezelése ezen alapelv szempontjából nagyon problematikus, mivel az irányelv 8. Cikkelye ilyen adatok esetén nem engedi a 7 (f) cikkelyben alkalmazott érdekkiegyenlítési technika (munkáltató jogos érdeke kontra munkavállalói alapvető jogok védelme) alkalmazását. Ez alól a szigorú tiltás alól az irányelv 8. Cikkely b. pontja jelent kivételt. Ennek értelmében, akkor kerülhet rá sor, ha az adatkezelőnek munkavégzésre vonatkozó tagállami jogszabály írja elő az adatkezelési kötelezettségét és megfelelően biztosított a munkavállalói jogok védelme.

f) Arányosság (proportionality)

Az arányosság elve nem más, mint egy arányosítás. Az egyik oldalon az adatgyűjtés és feldolgozás módszere áll, míg a másikon a minősítő értékek: adekvátság, relevancia és túlzás nélküli (megfelelő mennyiségű) adatgyűjtés. Az arányosság tehát azt jelenti, hogy a végzett adatgyűjtés akkor lesz megfelelő, ha az előre kitűzött célnak megfelel, csak releváns adatokat gyűjt és a cél eléréséhez szükséges mértéket nem lépi túl. Ezt az alapelvet nem lehet általánosítani. Szinte minden egyes munkáltatónál az adott körülményekhez, a munkáltatói érdekekhez viszonyítva kell meghatározni a tartalmát.

Az arányosság elve alapján nem fogadható el az a módszer, amikor a munkáltató minden egyes munkavállalójának a teljes e-mail/Internet forgalmát kontrollálja és nemcsak bizonyos célszemélyekre szűkítve, illetve korlátozott mértékig.

Amennyiben a munkáltató által elérni kívánt cél szempontjából is megfelelő, akkor az e-mail ellenőrzését úgy kell elvégezni, hogy a kontroll csak a forgalmazásra terjedjen ki és ne érintse a forgalmazott információkat vagy a levelek tartalmát. Amennyiben az e-mail levelezés tartalmának a megismerése elengedhetetlenül szükséges, akkor feltétlenül figyelemmel kell lenni arra a tényre, hogy a levelezés ellenőrzése során mind a saját (belső) munkavállaló (küldő személy), mind pedig a külső harmadik személy vagy esetleg egy másik (belső) munkavállaló személyiségi jogai ne sérüljenek. A munkáltató általában nem tudja beszerezni azon külső harmadik személyek beleegyező nyilatkozatát, akikkel a munkavállalói levelezéses kapcsolatban állnak. Ők a levelezésben érintett – külső, harmadik – személyek, de fölöttük a munkáltató semmilyen hatalmat nem gyakorol, sőt velük rendszerint semmilyen jogviszonyban nem áll. Ugyanakkor a munkáltatónak minden tőle telhetőt meg kell tenni azért, hogy ezeket a külső harmadik személyeket értesítse az ellenőrzés és megfigyelés tényéről. Erre azért van szükség, mert a munkavállaló e-mail forgalmának ellenőrzésekor ezen külső harmadik személyek személyiségi jogai is sérülhetnek, hiszen ők a levelezés másik oldalon lévő alanyai. A külső harmadik személyek informálását rendszerint úgy szokták megoldani, hogy a kimenő levelek aljára írnak egy figyelmeztető szöveget, ami tudatja a címzettel, hogy a levelezést megfigyelik.

A kollektív szerződések nagyon fontos szereplői lehetnek az „arányosság elvének" tartalmi meghatározásánál. A kollektív szerződésben rögzíthetik a felek, hogy a munkáltatónál leggyakrabban felmerülő kockázatokkal szemben az elektronikus kommunikáció területén mi tekinthető arányos munkáltatói magatartásnak. A kollektív tárgyalás tehát egyensúlyt teremthet a munkáltatói és a munkavállalói érdekek között.

g) Pontosság és az adatok megőrzése (accuracy and retention of data)

Az alapelv arra utal, hogy a munkavállalóról csak jogszerűen gyűjtött és pontos adatokat lehet feldolgozni és megőrizni. Az adatok megőrzésével kapcsolatban az alapelv kimondja, hogy az adatokat csak a szükséges ideig lehet megtartani, tárolni. Az e-mail/internet forgalom központi szerveren történő megőrzésének időtartamát a munkáltatónak kell meghatároznia. A gyakorlat azt mutatja, hogy általában a három hónapig őrzik az adatokat, utána megsemmisítik azokat.

h) Biztonság (security)

A munkáltató köteles olyan technikai és technológiai rendszert bevezetni, amely képes garantálni, hogy a gyűjtött és tárolt információk biztonságban legyenek és nem fenyegeti őket külső, jogtalan behatolás veszélye. A munkáltatónak tehát biztosítani kell a biztonságos adatfeldolgozás és megőrzés feltételeit. Ez az elv felhatalmazza a munkáltatót, hogy védje a rendszert illetéktelen külső behatásokkal – mint például a számítógépes vírus támadása stb. – szemben. Ez a jogosultság sok esetben azzal a kötelezettséggel jár, hogy a munkáltatónak a védelem biztosítása érdekében olyan automatikus ellenőrző rendszert kell felállítania, amely a munkahelyi e-mail/Internet forgalmat ellenőrzi. Ez pedig azonnal felveti a személyiségi jogok védelmének, illetve megsértésének a problémáját. Az EU szakértők azon az álláspontón vannak, hogy a munkavállalói e-mail/Internet forgalomnak az ilyen védelmi célú ellenőrzés alapvetően nem sérti a munkavállalók személyiségi jogait és a magánszféráját. A munkáltató tehát saját kockázatá-

nak a csökkentése és gazdasági érdekeinek a védelme érdekében anélkül használhat az e-mail-t/internetet automatikusan ellenőrző programokat, hogy ezzel megsértené a munkavállalók személyiségi jogait.[10]

A szabályozás során külön figyelmet kell szentelni a rendszergazdára. Ez a személy adatvédelmi szempontból nagyon fontos pozíciót tölt be. A rendszergazdára és minden más olyan személyre, aki a munkavállalók adataihoz hozzáférhet, a bizalmasan kezelt információk tekintetében nagyon szigorú titoktartási kötelezettség vonatkozik.[11]

1.3. Ajánlások az EU irányelv alkalmazásához és a továbbfejlesztéséhez

A különféle szakmai dokumentumokból és bizottsági üléseken elhangzottakból az EU-s irányelv továbbfejlesztésének alábbi koncepciója rajzolódik ki.

a) A munkavállalók képviselőinek bevonása

A munkavállalók képviselőit teljes körűen tájékoztatni kell minden bevezetendő olyan új információs rendszerről, amelynek a rendeltetése, hogy a munkavállalókat megfigyelje, róluk információkat gyűjtsön. A munkavállalói képviselőknek biztosítani kell, hogy bármikor meggyőződhessenek arról, hogy a munkahelyi belső szabályok rendelkeznek a munkavállalók személyiségi jogainak a védelméről. Rendszeres információcserét és tárgyalásokat kell folytatni annak érdekében, hogy olyan új információs technológiák kerüljenek bevezetésre, amelyek lehetővé teszik a munkavállalók személyiségi jogainak a védelmét. A munkahelyen működő információs rendszerekben jelentős változást csak a munkavállalók képviselőinek egyetértésével lehessen bevezetni.

b) A munkavállalók tájékoztatása

Az olyan munkahelyeken, ahol adatgyűjtés, illetve megfigyelés miatt elektronikus rendszereket (számítógéphálózat, audió-video rendszer, stb) alkalmaznak a munkavállalókat előre tájékoztatni kell az adatgyűjtés (megfigyelés) céljáról, a gyűjtött adatok felhasználásának módjáról és céljáról, az alkalmazott módszerről (technikáról, rendszerről), a gyűjtött adatok jellegéről, azon személyek köréről, akik ezekhez az adatokhoz hozzáférhetnek és annak a lehetőségéről, hogy miként eszközölhetnek helyesbítést a rendszer által gyűjtött adatokban, ha azok hibásak. A betekintéshez és az esetleges hiba esetén a kijavításhoz való jogot egy jól behatárolható időszakon belül kell biztosítani.

c) Tájékoztatás az alkalmazott technológiáról

A munkáltatónak informálnia kell a munkavállalóját a munkahelyen alkalmazott információs-rendszer tipizálásáról (pl. e-mail vagy hangposta, stb.) és azok felhasználási rendjéről. Ugyancsak informálnia kell a munkavállalót az adatgyűjtés és az adatok felhasználásának elveiről, céljáról és módszeréről.

[10] I. m. pp. 16–18.
[11] I. m. pp. 18–19.

d) A személyiségi jogok legitim elvárási szintje

A munkáltatónak tiszteletben kell tartania a munkavállaló személyiségi jogait. Létezik a munkavállaló személyiségi jogaival kapcsolatos legitim elvárási szint, amit tiszteletben kell tartani. Az elvárási szint megítélése minden esetben az adott munkahely sajátosságainak megfelelően alakul. Például az elvárási szint magasabb lesz egy zárt munkahelyen, mint egy nyitott munkahelyen.

e) Szükséges és indokolt adatgyűjtés

A munkahelyeken csak jogszerűen lehet adatot gyűjteni és felhasználni. Az adatok felhasználásának mindig korrektnek kell lennie és soha nem sértheti a munkavállalók emberi méltóságát. Az adatgyűjtésnek szükségesnek, arányosnak és adekvátnak kell lennie, amelyet a jóhiszeműség és a szakmai szükségesség vezérel. Az adatokat csak olyan mértékig és időtartamig lehet gyűjteni, amely az elérendő cél megvalósítása érdekében indokolható.

f) Személyhez köthető anyagok gyűjtése

Az adatgyűjtés során a munkáltatónak minden esetben ügyelnie kell arra, hogy tartózkodjon az olyan jellegű információk, adatok gyűjtésétől, amelyek nem kapcsolódnak közvetlenül a munkavégzéshez. Nem kapcsolódnak közvetlenül a munkavégzéshez azok az adatok, amelyek például a a munkavállaló személyes viselkedésére, személyiségjegyeire, vagy a munkahelyen belüli, illetve kívüli személyes kapcsolataira vonatkoznak.

g) A személyes adatok felhasználása a munkavállalóval szemben

A különböző módszerek segítségével összegyűjtött adatok nem használhatók fel a munkavállalókkal szemben. A munkavállalóról rendelkezésre álló adat csak abban az esetben használható fel vele szemben, ha a munkavállalónak előzetesen lehetősége volt arra, hogy ezeket az adatokat megismerje és szükség esetén korrigálhassa őket.

h) A munkavállalók rejtett megfigyelésének a tilalma

Csak kivételes esetben indokolható az olyan adatgyűjtés, illetve felhasználás, amelyről az érintett munkavállalónak nincs előzetes tudomása, illetve amely eltér az előre jelzett célkitűzéstől. Az információt az érintett személy előzetes és írásbeli belegyezésével lehet jogszerűen gyűjteni, illetve felhasználni. Ennek az írásbeli nyilatkozatnak a következő pontokat kell tartalmaznia: a) az okok és célok megjelölése; b) az összegyűjtendő információ természetére vonatkozó kitételek

Megjegyezzük, hogy az adatgyűjtésről, illetve felhasználásról nemcsak magát a munkavállalót, hanem a munkavállalói érdekképviseleteket is tájékoztatni kell.

i) „Megfigyeléstől mentes övezet (terület)" kijelölése

A munkáltatónak garantálnia kell a munkahelyen belül egy olyan tér létezését, ahol a munkavállaló személyiségi jogai semmilyen adatszerzéssel vagy megfigyeléssel nem

kerülnek veszélybe. Világosabban fogalmazva ez annyit jelent, hogy van a munkahelyen belül egy olyan tér (szoba, folyosó, stb.), ahol a munkavállaló szabadon - a megfigyelés veszélye nélkül – cselekedhet, például beszélgethet a munkatársaival, átöltözhet, stb.

2. *Az Európai Unió új adatvédelmi szabályozásának a koncepciója*

Az elmúlt időszakban az EU-ban többször megjelent az a törekvés, hogy a munkavállalók személyiségi jogait és méltóságát már a meglévő szinten túlmenően védjék. Például a Data Protection Working Party Opinion 8/2001 29. cikkelye, amely a foglalkoztatással összefüggő személyes adatok feldolgozásáról szól (Brüsszel, 2001. szeptember 13.), vagy a Social Policy Agenda of the Commission (COM2000/379 final, 28.6.2000), amely az alapvető szociális jogok tiszteletben tartásáról és fejlesztéséről szól, mert ez kulcsfontosságú tényező egy igazságos társadalom felépítéséhez, amelyben tisztelik az emberi méltóságot, beleértve a munkavállalók személyiségi jogainak a védelmét is.

A személyiségi jogok hatékony védelme szempontjából különbséget kell tenni az információ (adat) jogszerű (legitimate) és jogellenes (harmful) felhasználása között. Ezen cél megvalósítása közben egyensúlyt kell teremteni az információk szabad áramlása és a személyiségi jogok hatékony védelme között. Ebben az összefüggésben az adattovábbítás módjára is hangsúlyt kell helyezni. Amikor a személyiségi jogok védelméről van szó, akkor egy nagyon sokrétű és bonyolult szabályozási rendszer minden elemét kell egyidejűleg szem előtt tartani. Figyelembe kell venni a vonatkozó nemzetközi, regionális és tagállami jogi standardokat, valamit a munkáltatók belső szabályzatait. Ez a bonyolult szabályozási struktúra sok esetben inkább ellehetetleníti, mintsem segíti az adatok szabad áramlását. Ha csak az Európai Uniót vesszük alapul, akkor azt láthatjuk, hogy jelenleg a Közösségi szintű szabályozás (95/46/EC irányelv) végrehajtása tagállamonként eltérő és az irányelv végrehajtására alkotott normákon kívül még számos tagállami szabályozás létezik, vagy éppen az jelent problémát, hogy nem létezik megfelelő – a Közösségi szintű normával kompatibilis – szabályozás. Minden tagállam azt szeretné, ha a Közösségi norma egyenlő védelmet nyújtana mindenki számára. További cél, hogy mind a Közösségi irányelvet, mind a tagállami szabályozást egyszerűsíteni kell és a tagállamok saját szabályozását egymással konzisztens egységbe kell hozni. A Global Privacy Alliance (GPA)[12] résztvevői hisznek abban, hogy az egyszerűbb szabályozás létrehozása megkönnyíti az adatvédelemmel foglalkozó hatóságok feladatát. Ezáltal pedig lehetővé válik, hogy a kollíziós problémák megoldása helyett, vagy mellett nagyobb figyelmet szentelhessenek a személyiségi jogok védelmének.

Mint ahogy az a mindennapokban is érzékelhető, az elmúlt néhány évben – köszönhetően az Internet, az e-mail rendszereknek és a digitális műholdas technológiáknak – az adatok áramlása globális szinten óriási fejlődésen ment keresztül. Ez a globalizált adatáramlás a társadalom szinte minden egyes tagját érinti. Gondoljunk itt az interneten keresztül történő vásárlásra, vagy banki ügyletek intézésére, vagy az elektronikus kor-

[12] A GPA egy olyan szervezodés, amely különbözo ágazatok képviseloibol áll, amely azért jött létre, hogy globális szinten elosegítse az adatok szabad áramlását. Ezzel együtt felvállalta az adatáramlással kapcsolatban felmerülo adatvédelmi és személyiségi jogi problémák megoldását, növelve az adattulajdonosok bizalmát, az adatok szabad áramlását és az ezzel kapcsolatos gazdasági elonyöket. A teljesség igénye nélkül kiemelönk néhány ismertebb alapító vállalatot: Baxter International, Inc., Citigroup, Inc., General Motors Corporation, IBM Corporation, Oracle Corporation, The Procter & Gamble Company stb.

mányzás bevezetésére. A munka világát is jelentős mértékben áthatja az információs forradalom. A multinacionális vállalatok vezetéséhez elengedhetetlen, hogy a gazdasági és a humán erőforrással kapcsolatos információk pillanatok alatt eljussanak a világ egyik részéből a másikba. Ez nem lehetséges, ha a humán erőforrásokra vonatkozó adatokat tartalmazó adatbázisokat államonként elkülönülten hozzák létre. A multinacionális vállalatok, de a kisebb cégek működése is gyakorlatilag elképzelhetetlen a gyors és nagy mennyiségű adatáramlás megvalósulása nélkül. A multinacionális vállalatoknak gyakran kell válaszolniuk olyan kérdésekre, hogy összesen hány munkavállalójuk van, melyik milyen mobilitásra képes, milyen nyelvet beszél, milyen végzettsége van, stb. A rendszer nagyon nehezen lenne működtethető, ha minden egyes alkalommal államonként másmás rendszerben gyűjtött és feldolgozott adatokat külön-külön kellene kezelni. Gazdasági szempontból hasonló a helyzet. Egy multinacionális vállalatnak minden pillanatban tudnia kell a leltárkészletről, milyenek az értékesítési mutatók stb. A hatékony gazdasági működés érdekében az ügyfelek elvárják, hogy a cég 24 órán keresztül álljon a rendelkezésére. Gondoljunk például egy nemzetközi szállodaláncra. A potenciális vendég a világ bármely részéről, bármikor kérhet információt vagy szobát akar foglalni, stb. Ezt pedig csak úgy lehet megvalósítani, ha az egyes időzónák között szervezik meg a munkát. Ez folyamatos és naprakész információáramlást feltételez. Az elmúlt időszak egyik vállalatszervezési sajátossága az ún. out-sourcing - vagyis az egyes munkafeladatok kivitele a cég kereteiből valamely erre specializálódott másik céghez - szintén elképzelhetetlen folyamatos adatáramlás nélkül.

2.1. Az Európai Unió új adatvédelmi szabályozásának legfontosabb elemei

2002. október végén második szakaszában lépett az Európai Bizottság és a szociális partnerek hivatalos egyeztetése az európai munkavállalók személyes adatainak jövőbeni, fokozottabb védelméről.

Az Európai Bizottság a közelmúltban a szociális partnerek európai szervezeteinél (UNICE, ETUC, CEEPUAPME, Eurocadres stb.) egy sor, a személyes adatok munkahelyi kezelésére vonatkozó elvre és szabályra tett javaslatot, hogy ezáltal is világos iránymutatást adjon az európai munkavállalóknak és munkaadóiknak vonatkozó jogaikról, illetve kötelezettségeikről. A Bizottság döntése olyan, a munkahelyi adatvédelemmel kapcsolatos kérdéseket ölel fel, amelyeket első alkalommal 2001 augusztusában, az egyeztető folyamat kezdetekor vetettek fel a napirendre. Ezek között szerepel a bizalmas információk, a dolgozók egészségével, a velük elvégeztetett drog vagy genetikai tesztekkel kapcsolatos adatokat kezelése, valamint az elektronikus levelezés, illetve az Internet használatának felügyelete. Az egyeztető folyamat részeként a szociális partnereknek 6 hét állt a rendelkezésükre ahhoz, hogy a Bizottság ajánlásait véleményezzék, vagy adott esetben a kérdések rendezését a továbbiakban a Bizottságtól függetlenül folytassák, és önálló kezdeményezésekkel álljanak elő.

A konzultáció során a Bizottság hangsúlyozta annak szükségességét, hogy az Európai Unió mielőbb hatékony intézkedéseket hozzon a munkahelyi adatvédelem területén, és kialakítson egy európai szintű, elvi és szabályozási keretet. Az Európai Bizottság tudatában van annak, hogy a munkavállalók személyes adatainak kezelése sok esetben a munkáltató-munkavállaló kapcsolatának szükséges, és egyben ésszerű velejárója. Ez azonban kockázatokat is hordozhat a munkavállalókra nézve. Az Európai Unió tagállamai e kockázatokat igen eltérő módon értelmezik. A személyes adatok kezelésére vonat-

kozó szabályok sokfélesége sok esetben szükségtelen és nehezen áthidalható akadályokat gördít a belső piac működése elé. Ezzel egyaránt korlátozhatja a munkavállalók szabad mozgását, illetve a vállalatok azon lehetőségét, hogy a globalizált gazdaságban tevékenykedve szabadon áramoltathassák a dolgozóikra vonatkozó adatokat.

Az Európai Bizottságnak a szociális partnerekkel folytatott jelenlegi tárgyalásai mögött számos indok áll. Ezek között szerepel a technikai fejlődés (az elektronikus levelezés, illetve nyilvántartások; a távmunka terjedése, ami egyre inkább elmossa a munkavégzés (munkahely) és a magánélet (lakóhely) közötti határvonalat. Az egyre könnyebben hozzáférhető genetikai tesztek – ez utóbbiakat a munkáltatók sok esetben azért végeztetik el, hogy megítéljék érdemes-e a vizsgált személyt alkalmazniuk, illetve előléptetniük). A második ok maga a globalizáció: a nagyvállalatok humánerőforrás-menedzsmentjének kihelyezésre (out-sourcing) irányuló törekvése a vállalati hatékonyságra kedvező hatást gyakorolhat ugyan, de megvalósítása igen nagy nehézségekbe ütközik, ha az adatvédelem törvényi szabályozása országonként eltérő. Egyes államokban – ahogy az Egyesült Államokban is – a vállalatoknak adott esetben ellenőrizniük kell dolgozóik, illetve potenciális dolgozóik tevékenységét, összhangban a hatóságoknak a biztonság növelésére tett erőfeszítéseivel.[13]

A 2001-es tárgyalás eredményeként született meg egy EU-szintű keretmegállapodás. A szociális partnerek között széleskörű egyetértés volt a tekintetben, hogy valamilyen szabályozásra szükség van, ugyanakkor a nézőpontok még mindig meglehetősen eltérőek. A munkáltatói érdekképviseletek úgy vélik, hogy az Unió szintjén a jelenleg meglévő EU-s szabályozás (95/46/EC irányelv) alapvetően elegendő. Ennél részletesebb szabályokat a tagállami szinten kell megalkotni vagy munkahelyi szintű önkéntes megállapodás tárgyává lehetne tenni. A szakszervezetek álláspontja szerint a munkavállalói érdekek védelme nagyon rossz és a magánszféra védelmét tekintve kiszolgáltatott helyzetben vannak. A kollektív munkajog szemszögéből nézve a kérdést megállapítható, hogy a munkavállalói érdekképviseletek a kollektív tárgyalások során nagyon sokszor nem rendelkeznek megfelelő érdekérvényesítő képességgel. Az individuális munkajogi viszony keretében is megvan ez a kiszolgáltatott pozíciójuk, amikor az adatgyűjtést vagy megfigyelést „szentesítő" beleegyezési jogukat gyakorolják. A jelenlegi EU-s irányelvvel kapcsolatban meg kell említeni egy olyan hiányosságot, amely a további speciális jogalkotást indokolja. Az irányelv csak általános adatvédelmi szabályokat tartalmaz és nem rendezi a munkaviszony keretében felmerülő specifikus problémákat.

A Bizottság arra az álláspontra helyezkedett, hogy egy erős és világos jogi védelmi rendszert kell kiépíteni. Közösségi szinten egy teljes körű adatvédelmi normát kell elfogadni, amelyben az általános adatvédelmi elveken és szabályokon kívül a munkavégzésre vonatkozó specifikus elvek és szabályok is helyet kapnak. A Bizottság ennek az új Közösségi normának a jogszabályelőkészítési folyamatába meghívta a szociális partnereket, hogy mondják el a saját álláspontjukat és javaslataikat. A meghívás mögött az a cél húzódott meg, hogy remélhetőleg az érintett felek saját maguk képesek lesznek egy konszenzuson alapuló irányelv létrehozására.[14]

---

[13] http://europa.eu.int/comm/employment_social/news/2002/nov/181_fr.html

[14] Tökéletes példa ez az ún. horizontális szubszidiaritás gyakorlati érvényesülésére. A horizontális szubszidiaritás lényege, hogy a normaalkotás folyamatába a szociális partnerek – a normával érintett felek – is képesek legyenek beleszólni és az általuk leginkább fontosnak tartott kérdéseket megvitatni. Amennyiben konszenzus a vita eredménye, akkor ezt a megállapodást öntik jogi normába. Amennyiben nincs megállapodás, akkor a Bizottság fogja elindítani a kodifikációs folyamatot. 2001-ig gyakorlatilag három irányelv esetén

Az alábbiakban a keretmegállapodás részletes szabályait tárgyaljuk.[15]

2.2. *A szociális partnerek álláspontjai*

2.2.1. Háttérinformációk

Az Európai Bizottság először 2001. augusztus 27-én konzultációt kezdeményezett a szociális partnerekkel a munkavállalók személyes adatainak védelmére vonatkozó szabályozásról. A Római Szerződés 138. Cikkely 2. bekezdés alapján a szociális partnereket arra kérték, hogy nyilvánítsanak véleményt a Közösség e területre vonatkozó szabályozásának jövőbeni, lehetséges irányairól.[16] A második konzultációra 2002. október 30-án került sor. A Munkaügyi Kapcsolatok Általános Igazgatóinak (General Directors of Industrial Relations) találkozójára 2002. november 8-án, Korfun került sor. Itt a résztvevők többsége azon az állásponton volt, hogy a Közösségnek meg kellene alkotni egy keretnormát, amely a tagállamok számára megfelelő jogalkotási mintát és keretet jelentene. A kérdést ugyancsak megvitatták az egyes tagállamok szakértői 2003. március 10-én tartott ülésükön.

Az EU-ban jelenleg két irányelv vonatkozik az adatvédelemre. A 95/46/EC irányelv a személyes adatok feldolgozásáról és azok szabad mozgásának védelméről rendelkezik. A 97/66/EC irányelv a személyes adatok feldolgozásáról és a telekommunikációs ágazatban a magánszféra védelméről rendelkezik.[17] Ezek az irányelvek általános adatvédelmi szabályozást tartalmaznak és csak egy helyen található bennük a munkavállalásra vonatkozó speciális megközelítés. A Bizottság a normák végrehajtása és továbbfejlesztése érdekében megkérdezte a szociális partnereket, hogy a két irányelv megfelelő védelmet nyújt-e a munkavállalók számára. A szociális partnerek véleményét különösen az alábbi kérdésekben kérték ki és azt szerették volna megtudni, hogy kívánatosnak tartják-e, hogy a Bizottság további jogalkotási erőfeszítéseket tegyen ezekbe az irányokba:

a) Beleegyezés [kérdésként merült fel, hogy a fentiekben említett irányelvek alkalmazása során az érintett személy (jelen esetben munkavállaló) beleegyezése legitimizálja-e az adatok feldolgozásának munkáltató által választott módját és eszközét];
b) Egészségügyi adatok megszerzése és feldolgozása;
c) Munkajogi vonatkozású drog teszt és genetikai teszt;
d) Munkahelyi megfigyelés és ellenőrzés.

---

muködött a horizontális szubszidiaritás elve: a) szülési szabadság (parental leave); b) részmunkaido; c) határozott idore szóló munkaszerzodések kérdése. Ezen kívül a telemunkára vonatkozó irányelvet a szociális partnerek saját maguk hajtották végre (Lásd Social Agenda 3.).

[15] http://europa.eu.int/comm/employment_social/news/2002/nov/181_fr.html

[16] http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf; Second stage consultation of social partners on the protection of worker's personal data, p.2.

[17] Directive 95/46/EC of 24.10.1995, OJ L 281 of 23.11.1995, p. 31.; Directive 97/66/EC of 15.12.1997, OJ L 24 of 30.01.1998 p. 1. Lásd még: Regulation (EC) No. 45/2001 of 18 December 2000 concerning the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8 of 12.01.2001. p. 1.

Ezeken kívül még azt a kérdést intézték szociális partnerek felé, hogy milyen formában jelenjen meg a Közösségi normaalkotás (irányelv, ajánlás, viselkedési kódex (code of practice), irányelvek stb.[18]

2.2.2. A szociális partnerek válaszai

A szociális partnerek között széleskörű konszenzus alakult ki a tekintetben, hogy a személyes adatok védelmére vonatkozó szabályozásnak ki kell terjednie a munkahelyi viszonyokra is. A normaalkotásnál feltétlenül figyelembe kell venni a Közösség és az egyes tagállamok gazdasági és társadalmi körülményeit, valamint a technológiai fejlődés mindenkori állapotát. Ezek a kérdések közvetlen hatással vannak a munka minőségére és a munkahelyi szintű munkaügyi kapcsolatok alakulására.

A fenti közös ponton kívül a szociális partnerek válaszai és a témával kapcsolatos álláspontjai heterogén képet mutattak. Ugyanakkor nagyon tiszta különbség jelentkezett a munkáltatói és a munkavállalói érdekképviseletek álláspontja között. Míg az előbbi csoport alapvetően ellenezte, addig az utóbbi támogatta a jogi normákban (konkrétan irányelvekben) megtestesülő szabályozást.

A válaszolók közül néhány szociális partner úgy nyilatkozott, hogy ez egy nagyon bonyolult kérdés és a normaalkotás további menete kiterjedt kutatásokat kíván. Megjegyezték, hogy szoros összefüggés van az adatvédelmi szabályozás, a munkajog és a kollektív szerződések között.

A munkáltatói érdekképviseletek (UNICE, UEAPME, BDI) álláspontja szerint ezen a területen nincs szükség közösségi, irányelvi szintű szabályozásra. Álláspontjuk szerint a már létező Közösségi szabályozás (95/46/EC irányelv) megfelelően biztosítja a munkavállalók személyi adatainak a védelmét. Ugyanakkor a Közösségi szintű végrehajtás még korai szakaszában van. Véleményük szerint az új jogalkotási törekvések helyett sokkal inkább a végrehajtásra kellene a hangsúlyt helyezni és olyan átfogó tanulmányokat kellene készíteni, amelyek pontosan és naprakészen tükrözik az egyes tagállamok gyakorlatát.

Továbbá, minden munkáltatói érdekképviseleti szervezet a szabályozással szembeni elvárásként fogalmazza meg a rugalmasságot, nemzeti különbségek érvényre juttatását, valamint a túlszabályozás és a munkáltató további fölösleges feladatokkal való terhelésének az elkerülését.

Az UNICE és az UEAPME kihangsúlyozzák az áttekinthető szabályozás szükségességét. Különösen az UNICE szorgalmazza, hogy nemzeti szintű szabályozásnak áttekinthetőnek kell lennie, valamint a téma iránti érzékenység növelésére és a tagállamok között az információk és a jó gyakorlat (best practice) kölcsönös áramoltatására kell fokozott figyelmet szentelni.

Az UNICE álláspontja szerint ezeket a kérdéseket nemzeti szinten olyan nem kötelező normákba (non-binding instruments) kell foglalni, amelyeket előzetesen a szociális partnerekkel megvitattak. Az UEAPME véleménye szerint EU szinten is – az ILO vonatkozó viselkedési kódexének (Code of Conduct) az alapul vételével – nem kötelező erejű normában (non-binding instruments) – például nemzeti vagy munkahelyi viselkedési kódex – kell a kérdést szabályozni.

[18] http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf; Second stage consultation of social partners on the protection of worker's personal data, p. 2.

A másik oldalon viszont az összes munkavállalói érdekképviseleti szerv arra az álláspontra helyezkedett, hogy a kérdést Közösségi szintű kötelező normában – irányelvben – kell szabályozni. Kihangsúlyozták, hogy a meglévő adatvédelmi irányelvek nagyon hasznosak, de túlságosan általánosak és ezért a specifikus munkahelyi kérdésekre nem adnak adekvát választ. Az irányelvek végrehajtására kiadott nemzeti normák szintén nem fognak át minden – a munkaviszony szempontjából releváns – kérdést. Figyelembe véve azt a helyzetet, hogy egyre több munkavállaló dolgozik más tagállamban alapított munkáltatóknál, a személyek szabad mozgására és a diszkrimináció tilalmára vonatkozó Közösségi normaalkotás – különös tekintettel a Közösségen belül szabadon mozgó adatok védelmére – kívánatos tendencia.[19]

A Közösségi szintű normaalkotás akkor lehet megfelelő, ha bizonyos mértékű flexibilitást biztosít a nemzeti sajátosságoknak.

2.3. A Bizottság álláspontja

A munkavállalók személyes adatainak védelme folyamatosan vitatott kérdés. Ennek az oka alapvetően a következő tényezőkre vezethető vissza: *a)* elsősorban a munkavégzés alanyai között létrejövő munkajogviszony speciális természete, *b)* a globalizálódó világ társadalmi-gazdasági folyamatai, *c)* a munkaszervezetben bekövetkező változások és *d)* a technika – ezen belül is a kommunikációs technológiák – rohamos fejlődése.

Ténykérdés, hogy napjainkban a munkahelyen, illetve a munkavégzéssel összefüggésben – szinte rutinszerűen – nagyon sok személyes adat gyűjtésére, feldolgozására és kezelésére kerül sor. Ez nem szükségképen csak a munkáltató érdekében történik, hanem a munkavállaló saját érdekében is. A személyes adatok gyűjtése, feldolgozása és alkalmazása már a munkaviszony létrejöttét megelőzően elkezdődik (interjú, adatlapok, alkalmassági tesztek stb.), majd a jogviszony fennállása alatt is folytatódik, sőt – bizonyos esetekben – a jogviszony megszűnését követően is tart (pl. véleményezés kiadása stb.). Az adatgyűjtés legitimmé tételére számos út létezik. Ezek elsősorban arra adnak választ, hogy adott esetben miért lesz jogszerű az adatgyűjtés. A legfontosabb indokok a következők: *a)* jogszabály írja elő; *b)* az egészséges és biztonságos munkavégzés feltételeinek a megteremtése miatt szükséges; *c)* segíti a legmegfelelőbb jelentkező kiválasztását új munkaerő felvételekor, az iskolai beiskolázáskor és az előmenetel meghatározásakor; *d)* a munkaértékelés eszköze; *e)* a munka minőségének és a vevőszolgálat működésének ellenőrzése; *f)* bizonyos ellátásokra (jutalmazásra) való jogosultság eldöntéséhez nyújt segítséget.

A technológiai fejlődés eredményeként nagyon megnőtt annak a veszélye, hogy a munkavállalóról egyre több adatot lehet összegyűjteni, feldolgozni és felhasználni. A tapasztalat azt mutatja, hogy ezzel együtt általában megnövekszik annak az esélye is, hogy a munkavállaló alapvető emberi jogai – magánszféra védelméhez való jog – megsérülnek. Az egyre fejlődő és egyre olcsóbbá váló technológia magában hordozza annak a veszélyét, hogy az emberi jogok esetleg még tovább sérül(het)nek. Példaként hozzuk fel a genetikai teszteléshez kifejlesztett elektronikus chip-et. Az EU fejlettebb tagállamaiban a munkavégzés során is egyre jobban elmosódik a határ a munkahely és a magánélet között. Gondoljunk csak itt a telemunka intenzív terjedésére.

---

[19] I. m. p. 2–4.

A legfontosabb cél, hogy a jogszabályok, de még inkább fontos, hogy a részt vevő felek akaratának leginkább megfelelő és a felek számára kölcsönösen elfogadható egyensúlyt teremtsenek a két alapvető érdekellentét – egyrészt a munkáltató gazdasági érdekei, másrészt a munkavállaló emberi jogának – magánszférájának, személyiségi jogainak a védelmét szolgáló érdekei – között. Ennek az egyensúlynak a megtalálása teljesen szubjektív és mindenkor a felektől, azok gazdasági, társadalmi környezetétől, a társadalom kulturális sajátosságaitól, az emberi jogok érvényesíthetőségének mértékétől stb. függ. Ugyanakkor mindig felmerül egy normatív megközelítési mód is, amelyben a megoldandó dilemma abban áll, hogy szükséges-e a munka világára vonatkozóan megalkotni egy keret-iránymutatást (normatív alapelveket) és – a munkavégzés sajátosságait is tekintetbe vevő – további speciális jogi normákat.[20]

Mint azt már a korábbiakban említettük, a jelenleg hatályos két EU-s irányelvet (95/46/EC és a 97/66/EC irányelv) és hasonlóképpen a tagállamok belső jogalkotását egyaránt alkalmazni kell a munkavállalói adatok védelmére is. Hangsúlyoznunk kell, hogy ezek általános jellegű adatvédelmi szabályok és nem tartalmaznak a munkavállalókra vonatkozó specifikus szabályokat. Ezen adatvédelmi fő szabályok mellett meg kell említeni több Közösségi normát, amely a munkavállalókra vonatkozó adatokat érint.[21] Ezek elsősorban munkaegészségügy vagy munkabiztonsági tárgyú szabályozások.

2.4. A tagállami szintű szabályozás és a várható fejlődési trendek

Több tagállam felismerte, hogy személyes adatok védelme érdekében a meglévőnél részletesebb szabályozás szükséges, valamint azt is, hogy mind a tagállami általános adatvédelmi szabályozás, mind pedig a 95/46/EC irányelv végrehajtása során a munkavégzésre vonatkozó, azzal kapcsolatos specifikus szabályokat is be kell építeni a belső jogi normá(k)ba.

Az első tagállami szabályozás, amely átfogóan foglalkozik a munkahelyi adatvédelem kérdésével, az a 2001 májusában elfogadott finn törvény volt. A törvény kifejezetten előírta a munkavégzéshez kapcsolódó személyes adatok kötelező védelmét. A finn jogalkotók jelenleg azon dolgoznak, hogy az adatvédelmen túl, a munkavállalók személyiségi jogainak és magánszférájának a védelmét szolgáló jogi normát megalkossák.

Svédországban a személyes integráció védelmét szolgáló Bizottság (Committe on protection of personal integrity in working life) javasolta az illetékes svéd szerveknek, hogy fogadjanak el egy törvényt a munkavállalókra vonatkozó személyes adatok védelméről.

A tagállamok egy másik csoportjában[22] – a Közösségi Data Protection Supervisory Authorities ajánlásait követve, a munkavállalók személyes adatainak a védelmét szolgáló számos vélemény, ajánlás, viselkedési kódex jött létre. Megint más tagállamokban[23] ez a folyamat elkezdődött vagy legalább jogalkotási célkitűzésként már megjelent.[24]

---

[20] I. m. p. 4.

[21] Ezek közül a legfontosabbak a következők: Directive 89/391/EC on the introduction of measures to encourage improvements in the safety and health of workers at work, OJ L 183 of 29.06.1989, p. 1.; Directive 98/24/EC on protection of the health and safety workers from the risk related to chemical agents at work, OJ L 05.05.1998. p. 11.

[22] Belgium, Franciaország, Görögország, Hollandia, Egyesült Királyság.

[23] Németország, Írország, Portugália.

[24] http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf; Second stage consultation of social partners on the protection of worker's personal data, p. 6.

A tagállamok részletes szabályozását a későbbiekben tárgyaljuk.

2.5. Nemzetközi kezdeményezések

A 108. Számú Egyezményt követően az Európa Tanács (Miniszterek Tanácsa) elfogadta az R(89)2 Ajánlását, amely speciálisan a munkavégzés során használt személyes adatok védelméről rendelkezik.

Az ILO 1996-ban fogadta el a Viselkedési Kódexét (Code of Conduct), amely átfogóan foglalkozott a munkavállalók személyes adatainak a védelmével. Az Európai Közösség – később tárgyalandó – keretmegállapodása a munkavállalók személyes adatainak a védelméről leginkább ebből az ILO-s forrásból táplálkozik.

Az Európa Tanács által elfogadott Emberi Jogokról és a Biomedicináról szóló Egyezményt[25] követően Strasbourgban jelenleg a Humán Genetikai Protokoll kidolgozását végzik, amely a munkavégzéshez kapcsolódó genetikai tesztre vonatkozó speciális szabályozást is tartalmaz.[26]

2.6. A jogi szabályozás és a kollektív szerződések kérdése

A munkavállalók személyes adatainak védelmére vonatkozó szabályozás nemcsak Az adatvédelmi szabályozásban jelenik meg. Az adat természetétől függően szabályozás található még az alkotmányjogban, munkajogban, telekommunikációs jogban, stb. Ezen kívül a bírói esetjog és bizonyos esetekben a kollektív szerződéses szabályozás is meghatározó lehet. Az alkotmányjogban és a munkajogban rendszerint általános és elvi szintű szabályozásra kerül sor. A bírói esetjogban pedig egy-egy konkrét esetre vonatkozó nagyon konkrét probléma megoldására találhatunk választ. A jogi normák és esetjog interakciója tehát nem minden esetben eredményez tökéletes megoldást. Ezért jól definiálható a feladat: létre kell hozni egy olyan szabályt, amelyben átfogóan rendezhető a munkavállalók személyes adatainak a védelme.

További probléma, hogy a munkavállalók személyes adatainak védelme esetén a tagállami szabályozás – beleértve a jogszabályi és a kollektív szerződésekkel történő rendezést – a saját belső logikájára és történeti tradíciójára épül, amely nem minden esetben egyezik meg a többi tagállam jogi szabályozásával. Abban is különbség van, hogy az egyes tagállamok mennyi figyelmet szentelnek ezekre a kérdésekre.[27]

2.7. Az EU szabályozás szükségessége

Az EU tagállamok normaalkotását és joggyakorlatát áttekintve a Bizottság úgy látja, hogy kialakult egy világosan látható trend. Ennek a lényege, hogy tisztázni kell, vajon az általános adatvédelmi szabályozási elvek és szabályok alkalmazhatók-e a specifikusnak számító munkavégzési jogviszonyokra. Hasonló kérdésfelvetéssel találkozhatunk más nemzetközi szervezeteknél, amelyek ezzel a kérdéssel foglalkoznak. Az eddigi tapasztalatok azt mutatják, hogy jelentős igény mutatkozik arra, hogy az általános adatvédelmi

[25] Az Egyezményt az Európa Tanács Miniszterek Bizottsága fogadta el 1996 novemberében, majd 1997. Áprilisában írták alá Oviedoban.

[26] http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf; Second stage consultation of social partners on the protection of worker's personal data, p. 6.

[27] I. m. pp. 6–7.

szabályozáson kívül legyen specifikus – munkavállalói személyes adatok védelmére vonatkozó – szabályozás is. A jelenleg uralkodó álláspont szerint ezt egy EU-szintű keretmegállapodásban lehet leginkább megvalósítani.

A gyakorlatban azt láthatjuk, hogy néhány tagállamban az általános adatvédelmi elveket és szabályokat különféle értelmezések útján igyekeznek a munkavégzésre is alkalmazni. Ez némely esetben előre pontosan nem látható negatív következménnyel – bizonytalanság, ellentmondás stb. – is járhat. Más tagállamokban, ahol már van ugyan külön munkaviszonyban álló személyekre vonatkozó specifikus szabályozás, de ez(ek) normá(k) rendszerint nem átfogóan, hanem fragmentáltan szabályozzák a kérdéseket. Például néhány tagállamban csak a munkaerő felvétellel kapcsolatos adatvédelmet szabályozzák. Más tagállamokban csak az egészségügyi adatok kezelésére van szabály, de gyakran még ezekben a specifikus normákban sem rendelkeznek a drogtesztből és genetikai vizsgálatokból származó adatokról.

Számos érv szól a Közösségi szintű keretmegállapodás létrehozása mellett. A legfontosabb általános érvényű indok: *a)* jogbiztonság megteremtése (világos és biztos elveken nyugvó szabályozás), *b)* a Közösség államain belül is konzisztens és egységes szabályozás kialakítása, *c)* a munkaviszonyból eredő speciális sajátosságok érvényre juttatása, d) a technológiai fejlődésből eredő előnyök alkalmazása a munkahelyi viszonyok között.

Néhány további speciális érv ismert még:

a) A munkakörülmények javítása. A Római Szerződés 137. Cikkelye alapján a Közösség köteles mindent megtenni – beleértve a jogalkotást is –, hogy a tagállamok képesek legyenek megvalósítani ezt a célkitűzést. Konkrét példaként hozható fel a drog és genetikai tesztek vonatkozásában megalkotott speciális standardok. Ezek a standardok elsősorban a gyűjtött adatok legitimitására és minőségére vonatkoznak. Felfogásukban a legitimitás megteremtéséhez nem elegendő az érintett személy belegyezése, sőt a beleegyezésnek csak limitált, vagy bizonyos esetben egyáltalán nem jut szerep. Meghatározott adatok esetén a tagállami adatvédelmi szervezeteknek kötelességük az előzetes ellenőrzés. A magánjellegű e-mail fokozott védelme, függetlenül attól, hogy a munkáltató gépén történik és attól is függetlenül, hogy a munkáltató a munkahelyi számítógépes rendszerek magáncélú használatát szigorúan megtiltotta. Nagyon fontos még az a törekvés, hogy a szabályozás nagyon világos és egyértelmű legyen, mert ez a tagállami jogalkotás és jogalkalmazást javítja; növeli a jogtudatot (ezen a téren kinek milyen jogai és kötelezettségei vannak) és biztosítja a hatékony jogvédelmet.

b) A keretmegállapodás lehetővé teszi a személyes adatok védelmét a Közösség egész területén és teljes körűen biztosítja a személyhez fűződő jogokat és a magánszféra védelmét, mint alapvető emberi jogot. Ezen kívül lehetővé teszi a Közösségen belül az egységes és koherens jogi szabályozás megalkotását.

c) A személyes adatokra vonatkozó szabályozás tagállamonként eltéréseket mutat. Közösségi szintű, általános keretet jelenleg a 95/46/EC irányelv jelent. A személyes adatok védelmére vonatkozó közös európai elvek és keretszabályozás az információk szabad mozgásának a megteremtésével elősegíti az egyik legfontosabb Közösségi szabadságelv – a személyek szabad mozgásával – zavartalan érvényesülését. Más megközelítésben ez magas szinten védi a munkavállalók alapvető jogait és a szabadságát az EU-ban.

d) Az általános adatvédelmi elveket és szabályokat tartalmazó 95/46/EC irányelvet tovább kell fejleszteni, méghozzá abban az irányban, hogy képes legyen a munkavégzés

során felmerülő speciális adatvédelmi problémák kezelésére. Az új Közösségi szabályozással a jogi védelem előterébe kell helyezni a munkavállalók alapvető emberi jogait és szabadságjogait. A Közösség által alkotott *„A munkavállalók alapvető jogairól rendelkező karta (1989)"* számos pontjában utal a munkavállaló magánszférájának a védelmére.

e) A Közösségi keretmegállapodás azért is fontos, mert mintaként szolgál a csatlakozásra váró országok jogalkotása számára.[28]

2.8. A keretmegállapodás várható tartalma

2.8.1. A megállapodás hatálya és jogi tartalma

Megszilárdult álláspont, hogy a 95/46/EC irányelv rendelkezéseit a munkavállalók személyes adatainak a védelmére is alkalmazni kell. A két norma személyi hatályában nincs eltérés. Ezért az új keretmegállapodás kidolgozásakor nem az az alapvető cél, hogy a személyes adatok Közösségi szintű szabad áramlását kidolgozza, hanem az, hogy a már meglévő irányelv elveit és szabályait még pontosabban hozzáigazítsa a munkavégzés speciális viszonyaihoz. Ahol a munkaviszony sajátosságai megkövetelik, ott az is előfordulhat, hogy új rendelkezésekkel kell bővíteni az irányelvet.

Más adatvédelemre vonatkozó EU-s normákról – pl. 97/66/EC irányelv stb. – szintén elmondható, hogy a személyi hatályuk alapvetően kiterjed a munkavállalók kategóriájára is.

A keretmegállapodás tárgyi hatályának alapvetően meg kellene egyeznie a 95/46/EC irányelvben foglaltakkal. Az irányelv tárgyi hatálya kiterjed mindennemű információ feldolgozására, függetlenül a média fajtájától, beleértve a hangtovábbítást és a képi adatokat is. Azt is fontos kiemelni, hogy a keretmegállapodás nemcsak a már fennálló munkaviszony alatt keletkező információk feldolgozására terjed ki, hanem alkalmazni kell a munkaerőfelvétel során szerzett és a munkaviszony megszűnését követően még rendelkezésre álló adatokra is. A norma nemcsak a munkáltató adatfeldolgozási tevékenységére terjed ki, hanem egyaránt alkalmazni kell a munkavállalói érdekképviseletek, vagy munkaügyi hivatalok, munkaközvetítők stb. által végzett adatkezelésre is.[29]

2.8.2. A szabályozás alapvető elvei

a) Az Európai keretmegállapodás a 95/46/EC irányelv alapelvein nyugszik. Annyiban haladja meg azt – pontosítja és kiegészíti –, amennyiben a munkavállalói statusra, illetve a munkaviszonyra tekintettel szükséges.

b) Az Európai keretmegállapodás a munkavégző személyhez kapcsolódó mindennemű személyes adat és információ védelmére kiterjed.

c) Rendelkezéseit mind a magán, mind pedig a közszférában alkalmazni kell.[30]

---

[28] I. m. pp. 8–9.
[29] I. m. p. 9.
[30] I. m. pp.9–10.

2.8.3. Az Európai Keretmegállapodás többletszabályai

Mint a fentiekben láthattuk, a korábbi Közösségi irányelvek és a Keretmegállapodás rendelkezései túlnyomó részükben megegyeznek. Ugyanakkor található néhány olyan rendelkezés, amelyben a Keretmegállapodás bővebb.

a) A Keretmegállapodás tárgyi hatálya kiterjed minden manuálisan feldolgozott adatra, beleértve az olyan nem automatizált adatfeldolgozást, amely nem része a nyilvántartási rendszernek (filing system).

b) Amikor ez kívánatos, akkor a Keretmegállapodás tárgyi hatálya kiterjed a munkaügyi hivatalok és egyéb, a munkaerő-közvetítéssel foglalkozó szervezetek adatfeldolgozási tevékenységére, továbbá a munkavállalói érdekképviseleti szervezetek adatkezelésére.

A Keretmegállapodás értelmében a munkavállaló fogalma kiterjed: *a)* a munkaviszonyban álló személyre, *b)* a munkára jelentkezőre és *c)* a volt munkavállalóra.

2.8.4. A munkavállalói érdekképviseletek bevonása

Igaz ugyan, hogy a munkavállaló személyes adatainak a védelme alapvetően individuális jogi megközelítés kérdése, de a munkaviszonyban benne rejlő speciális viszonyrendszerben a kollektív érdekvédelemnek – ami elsősorban a munkavállalói érdekképviseletek feladata – meghatározó szerep jut. A kollektív érdekérvényesítés alapvetően kiegészíti a munkavállalónak az információhoz és az adatvédelemhez kapcsolódó individuális jogait. Az érdekvédelem hatékonysága rendszerint a szociális partnerek erőviszonyaitól függ. Ezért nagyon fontos, hogy a normaszöveg kialakításánál a szociális partnereket is be kell vonni a tárgyalásokba. A tagállami jogszabályok vagy gyakorlat mondják meg, hogy kik a munkavállalói érdekképviseletek.

A munkavállalói érdekképviseletek jogai tagállamonként kerülnek szabályozásra és ezért rendszerint tagállamonként eltérőek. A jogosultság magában foglalhatja a munkavállalók magánszféráját érintő kérdésekben a tájékoztatáshoz való jogot, vagy a konzultáció jogát vagy a szerződéskötés jogát. A Keretmegállapodás előírja, hogy a munkavállalók érdekeinek minél szélesebb körű védelme érdekében kívánatos, hogy a munkavállalók magánszféráját és személyiségi jogait érintő intézkedések, ellenőrzésre, illetve megfigyelésre szolgáló rendszerek bevezetése vagy módosítása előtt informálják és/vagy konzultáljanak a munkavállalók érdekvédelmi szervezeteivel. Ez különösen a következő intézkedések meghozatala előtt indokolt: *a)* olyan automatikus rendszerek bevezetése, amely a munkavállalók személyes adatait dolgozza fel; *b)* bármely olyan technikai eszköz beszerzése és beszerelése, amely a munkavállalók megfigyelésére és ellenőrzésére szolgál; *c)* a munkaerő-felvétel során vagy a munkavégzés során a munkavégzéssel kapcsolatos kérdőív és teszt minden formája, különösen az egészségügyi, genetikai, személyiségi teszt.

2.8.5. Az adatfeldolgozásra vonatkozó általános szabályok

A Keretmegállapodás alapvető filozófiáját meghatározó elveknek a 95/46/EC irányelv alapelveire (6. cikkely) kell ráépülnie. Ezért nem kell a már meglévő elveket újra kitalálni és szabályozni. Ugyanakkor a már meglévő alapelvek gyakorlati alkalmazása sem

mindig problémamentes. Például, a munkáltatók többsége még mindig abban a téves feltevésben van, hogy a munkavállaló beleegyezése jogszerűvé teszi a munkáltatói intézkedések összességét, még azokat is, amelyek egyébként nyíltan és nyilvánvalóan sértik a munkavállaló személyhez fűződő jogait. Például, sok munkáltató úgy gondolja, hogy amennyiben a munkavállaló beleegyezett akkor – függetlenül a betöltendő vagy betöltött munkakörtől – kérhető a munkavállalótól a rá vonatkozó teljes körű egészségügyi, vagy bűnügyi nyilvántartási adatot, vagy a beleegyezés lehetővé teszi, hogy a munkáltató rutinszerűen és folyamatosan megfigyelje a munkavállaló e-mail/Internet (beleértve a magánjellgű e-mail) forgalmának a tartalmát, stb. A Keretmegállapodás filozófiája szerint ez egyáltalán nem tekinthető általános érvényű elvnek, hanem minden esetben az adott helyzethez kell igazítani a munkáltató lehetőségeit. Jó példaként hozható fel erre a Finn Adatvédelmi törvény rendelkezései.

A munkavállaló beleegyezése a munkavégzés során végzett adatfeldolgozás/kezelés során – beleértve a harmadik országba történő adattovábbítást is – mintegy legitimáló szerepet tölt be. Ez – a munkavállaló alárendelt és kiszolgáltatott helyzetére tekintettel – egy meglehetősen vitatható koncepció. Például Belgiumban, ahol alapvetően tilos az ún. érzékeny személyes adatok feldolgozása, kivéve, ha az érintett munkavállaló(k) kifejezett beleegyezését adja ehhez. Ez az egyetlen kivétel létezik. Ettől eltérően a finn szabályozás kimondja, hogy a munkavállalók személyes adatainak a feldolgozása csak akkor végezhető el, ha az adott állás betöltéséhez, előmenetelhez, stb. kapcsolódóan arra szükség van (relevance requirement). A jogszabály nagyon szigorú és a relevancia elv alól nem enged kivételt, még a munkavállaló beleegyezése esetén sem. Vannak olyan országok, ahol a munkavállalói beleegyezés alapvetően legitimál, kivéve néhány – jogszabályban külön nevesített – speciális adatot.

A Keretmegállapodásba bele kell foglalni, hogy amikor indokolt és jogszerű a személyes adatgyűjtés célja. A korrekt adatgyűjtés elve azt kívánná meg, hogy az adatot vagy információt közvetlenül magától a munkavállalótól szerezzék be. Természetesen erre csak a munkavállaló előzetes hozzájárulásával kerülhetne sor.

2.8.6. A keretmegállapodás leendő alapelvei a következő pontokban összegezhetők:

a) A munkavállalók személyes adatai csak akkor kezelhetők, ha az releváns és szükségképpen kapcsolódik a munkavégzéséhez.

b) A személyes adat csak olyan célra használható fel, amelyre eredetileg gyűjtötték. Az adatfelhasználás az eredeti célkitűzésen nem terjeszkedhet túl. A munkavégzéshez kapcsolódó személyes adatok esetén meg kell fontolni, hogy mely esetekben kell még külön engedélyt kérni az illetékes hatóságtól (Supervisory Authority).

c) Az adatkezelést korrekt módon kell végezni. A munkaviszony keretei között ez azt jelenti, hogy az adatot attól a munkavállalótól kell beszerezni, akire az adat vonatkozik. Amennyiben mégis szükség van a harmadik személytől történő adatgyűjtésre, olyankor az érintett munkavállalót előre tájékoztatni kell és be kell szerezni a beleegyezését.

d) Biztosítani kell, hogy akire az adat vonatkozik korlátozás nélkül hozzájuthasson a róla gyűjtött információkhoz. A „munkaviszonnyal összefüggésben" feltételnek van egy olyan vetülete, hogy a munkáltató nem kérheti a munkára jelentkezőtől vagy a már tényleges munkavállalójától, hogy szerezzék be a saját magukra vonatkozó információkat – például egészségügyi vagy bűnügyi nyilvántartásban szereplő adatokat – azért, hogy azt utána a munkáltatóhoz továbbítsák.

e) Praktikus okokból a munkáltatónak kerülni kell az olyan megoldásokat, amikor az adatgyűjtés legitimitását a munkavállalótól kapott beleegyező nyilatkozat adja. A munkaviszony keretei között ez azért problematikus, mert a munkavállaló rendszerint egzisztenciálisan kiszolgáltatott helyzetben van az adatot gyűjtő munkáltatóval szemben, következésképpen a beleegyezésnél szabad akaratnyilvánítása megkérdőjelezhető. A beleegyező nyilatkozat helyett a 95/46/EC irányelv 7. cikkelyében foglalt módszerek, illetve elvek alkalmazására kell törekedni. Az általános alapelveken túlmenően a leggyakrabban használt elvek a következők: *a)* relevancia (relevance); *b)* szükségesség (necessity); *c)* arányosság (proportionality).

f) A személyes adatokat jogszerűen kell feldolgozni. Munkajogi vonatkozásban ez azt jelenti, hogy a munkavállalóról összegyűjtött adatok feldolgozásának nem lehet olyan célja vagy eredménye, amely a munkavállalóra nézve diszkriminatív vagy a munkavállalót egyéb módon hátrányos helyzetbe hozza.

g) Külön jelezni kell, hogy a munkavállalóról nem rendszeresen összegyűjtött adatot mely esetben lehet a munkavállalóval szemben – pl. bírósági eljárás stb. – felhasználni.

h) A munkaerő-felvételnél a speciálisnak (érzékenynek) minősített személyes adatokat – pl. egészségügyi adatok, bűnügyi adatok stb. – csak azután lehet kérni, ha a jelentkezők közül a képzettségük, jártasságuk stb. alapján már kiválasztották a potenciális jelentkezőt.

i) Elektronikus adatgyűjtés esetén meg kell határozni, hogy milyen biztonsági intézkedések kerülnek bevezetésre annak érdekében, hogy illetéktelen személyek az adatokhoz ne férhessenek hozzá. A biztonsági alapelvnek megfelelően a jogosultsággal rendelkező személyek statusát, feladatait és jogosultsági körét meg kell határozni. Az ún. érzékeny adatok kezelése esetén az adatkezelésre jogosult személyek számát minimálisra kell csökkenteni.[31]

2.8.7. Egészségügyi adatok

Alapvetően az egészségre vonatkozó adatok feldolgozása tilos. A tiltás oka, hogy ezek az adatok jelentős mértékben érintik az egyén magánszféráját. A munkaviszony keretében az egészségügyi adatok kezelése számtalanszor szükséges, amelyet a legtöbb esetben a jogviszony két alanyának kölcsönös érdekei alapján szoktak indokolni. Az általános tiltás alól számtalan kivétel található.

Az adatvédelem általános alapelveinek érvényesülése a munkaviszonnyal összefüggő egészségügyi adatok kezelése során:

– Munkaviszony keretében a személyes (egészségügyi) adatok csak a jogszabályban meghatározott esetekben és a jogszabályi garanciák betartása mellett kérhetők;

– Csak a munkavégzéshez szükséges esetben lehet kérni. Mikor szükséges: *a)* annak a kiderítésére, hogy a munkavállaló egészségügyi szempontból képes-e az adott munkakört ellátni; *b)* a munkahelyi munkaegészségügyi és munkabiztonsági feltételeknek megfelel-e; *c)* annak a megállapításához, hogy vajon a szociális biztonsági ellátásokra jogosult-e a munkavállaló.

– Az egészségügyi adatokat csak egészségügyi szakemberek vagy olyan személyek kezelhetik, akikre kiterjed az egészségügyi titoktartásról rendelkező jogszabály. Az egészségügyi adatokat a többi adattól elkülönítetten kell kezelni.

[31] I. m. pp.10–11.

– Egészségügyi vizsgálat esetén a munkáltatót csak a vizsgálat eredményéről és arról is csak annyiban kötelesek informálni, ami az esetleges munkáltatói döntéshez szükséges. Például, a munkavállaló az adott munkakört elláthatja vagy a munkavállaló az adott munkakört nem láthatja el vagy további rehabilitációs jellegű átalakítás szükséges a munkakörben stb.[32]

2.8.8. Az egészségügyi adatokon kívüli egyéb speciális (érzékeny) adatok

A 95/46/EC irányelv az adatok egy speciális kategóriáját sorolja fel. Ezeket ún. érzékeny adatoknak hívja a szakirodalom. Az irányelv a következő adatokat sorolja ebbe a körbe: *a)* faji vagy etnikai eredet; *b)* politikai nézet; *c)* vallás vagy világnézet; *d)* szexuális élet és *e)* büntetett előéletre vonatkozó adatok. Azért minősülnek ezek ún. érzékeny adatoknak, mert amennyiben ezeket a kérdéseket felteszik és a megkérdezett személy(ek) válaszolnak rá, akkor fennáll annak a veszélye, hogy az információk ismeretében a válaszolókat diszkriminálhatják. Ez a veszély a munkaviszony keretében szerzett adatok esetén is fennáll.

Az antidiszkriminációs törvények értelmében bizonyos érzékeny adatok, mint például a faji vagy etnikai eredet vagy vallás vagy világnézet csak különösen indokolt esetben – speciális szakmai követelmények vagy pozitív akciók[33] – kérdezhető meg.

Figyelembe véve a büntetett előéletre vonatkozó nyilvántartást, több tagállamban előírják, hogy amennyiben a munkáltató ilyen adatot kíván kérni a munkavállalójától, mielőtt ezt megtenné ajánlatos előzetes ellenőrzésre a tagállami Felügyeleti Szervhez (Supervisory Authority) fordulni.

Az érzékeny adatok kezelésére vonatkozó speciális alapelvek:

a) Az érzékeny adatok gyűjtése alapvetően tilos. Kivételes esetben, de akkor is csak külön jogszabályi felhatalmazás alapján lehet ilyen adatokat gyűjteni. Ezek a jogszabályok pontosan rendelkeznek az érzékeny adatok védelmére vonatkozó speciális szabályokról. Az adatvédelem alapelveit – az érzékeny adatokra tekintettel – a munkajogviszonyra a következőképpen lehet értelmezni.

b) a szexuális életre vonatkozó kérdést – ha erre feltétlenül szükség van - akkor lehet feltenni, ha például egy szexuális zaklatásos ügyben a munkáltató felelősségének megállapításáról van szó.

c) erkölcsi bizonyítványt (büntetlenség igazolása) akkor lehet kérni, ha az adott munkakör jellege és természete szükségessé teszi és a tagállami Felügyeleti Szerv (Supervisory Authority) a körülmények teljes körű mérlegelését követően, de még az adat bekérését megelőzően hozzájárult. A munkavállalótól még beleegyezése esetén sem lehet általában a büntetőjogi előéletére (bűnügyi nyilvántartásban szereplő adatok) vonatkozó kérdést feltenni.

d) szakszervezeti tagságra utaló adatot a vonatkozó jogszabály vagy kollektív szerződés által megszabott keretek között lehet gyűjteni. Ilyen esetben a jogszabály különböző védelmi szabályt ír elő. Például, a munkavállaló előzetes beleegyezése szükséges vagy a munkavállalónak vétó joga van.

e) A faji vagy etnikai eredetre, illetve vallásra vagy világnézetre utaló adatot csak jogszabály alapján lehet kérni. A jogszabály alapvetően két esetben enged kivételt: a)

[32] I. m. pp.13–14.

[33] Lásd bővebben a 2000/43/EC Irányelvet.

speciális szakmai követelmények vagy b) előnyben részesítési követelmény (pozitív akciók) esetén.[34]

2.8.9. A drog-tesztből származó adatok

A drog-teszt nagyon súlyosan érinti a munkavállaló magánszférájának a védelméhez fűződő jogát. Nemcsak maga a teszt, de a teszt eredménye is tartalmazhat ún. érzékeny adatokat. További fontos kérdés, hogy milyen legyen a drog tesztet gyakorisága és jellege: *a)* általános jellegű és szisztematikus teszt vagy *b)* eseti jelleggel, külön indok nélkül elvégzett beavatkozás.

A drog-teszt nem kizárólag a drog, hanem az alkoholfogyasztásra is kiterjed. Az alkohol és a drog-teszt között egy nagyon fontos különbség található. Pozitív alkohol-teszt esetén egyértelmű, hogy a munkavállaló az adott pillanatban nem alkalmas a munkavégzésre. Ugyanakkor a pozitív drog-teszt nem pusztán a vizsgálat időpontjára határozza meg a vizsgált személy drogfogyasztását, hanem arra utal, hogy a személy a múltban drogot fogyasztott. Tehát elképzelhető, hogy a vizsgálat időpontjában – ez rendszerint egybeesik a munkavégzési kötelezettség idejével – az illető személy már nem áll drog befolyása alatt. A drog-teszt nem utal múltbeli vagy jelenlegi megbetegedésre vagy ennek a kockázatára és ugyancsak nem utal a függőség kialakulására sem.

Milyen jogszerű érdekek húzódnak meg a drog teszt mögött. A munkáltató oldalán számos indok kimutatható: *a)* fitt és munkaképes munkavállalókat kíván, akik a legjobban teljesítenek; *b)* munkabiztonsági szempontból, a munkáltató felelősségét befolyásoló tényező. Ezen kívül természetesen számos népegészségügyi indok is található.

A gyakorlatban az ún. biztonságorientált munkáknál (safety-sensitive job) (például, közlekedés, magasépítés stb.) fordul elő a leggyakrabban az eseti jellegű vizsgálat.

A drog-teszt nem lesz jogszerű, ha annak alkalmazása nem indokolt, vagyis nincs megfelelő és alapos gyanú, arra nézve, hogy a drogot fogyasztó munkatárs e magatartásával munkatársának vagy külső harmadik személynek a biztonságát veszélyezteti.

A vizsgált személy beleegyező nyilatkozatát nem lehet úgy tekinteni, mint ami legitimálja a tesztből származó adatok feldolgozását.

Arra is figyelmet kell fordítani, hogy a teszt érvényes és hiteles legyen, valamint pontos adatokat tartalmazzon. Ennek az egyik záloga, ha a vizsgálatot szakemberek, a megfelelő szakmai előírások pontos betartásával végezzék. A drog-teszt eredményét – a benne rejlő ún. érzékeny adatok miatt – minden esetben bizalmasan kell kezelni.

A drog-teszttel kapcsolatos specifikumok a munkaviszonyban

a) Drog- (alkohol-) tesztet csak olyan célból szabad elvégezni, hogy kiderüljön az eredményből, hogy a munkavállaló alkalmas vagy sem az adott munkakör betöltésére. Képes-e a munkáját biztonságosan elvégezni, úgy hogy sem a munkatársai, sem pedig külső harmadik személyek testi épségét és biztonságát nem veszélyezteti.

b) Annak érdekében, hogy a tesztből származó adat gyűjtése és feldolgozása korrekt legyen, le kell szögezni, hogy csak a különösen biztonság-érzékeny (safety-sensitive) munkakört betöltő személyeknél lehet alkalmazni. Az egyéni drog-tesztet csak akkor lehet elrendelni, ha alaposan feltételezhető, hogy a vizsgálandó személy drogot fogyaszt

[34] http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf; Second stage consultation of social partners on the protection of worker's personal data, p. 12–13.

és ezzel a magatartásával jelentősen veszélyezteti a munkatársai vagy külső harmadik személyek biztonságát.

c) A drog-teszt adatait ún. önkéntes programok (voluntary programme) keretében is gyűjthetők és feldolgozhatók. Ezek fő célkitűzése a drogfogyasztásból eredő káros következmények enyhítése.

d) A drog-teszt adatait csak olyan egészségügyi szakemberek gyűjthetik és kezelhetik, akik az egészségügyi titoktartásra vonatkozó jogszabály hatálya alá tartoznak.[35]

2.8.10. Genetikai teszt

A genetikai teszt nagyon komolyan érinti a vizsgálat alanyának és az azonos genetikai vonalhoz tartozó családtagjainak a személyiségi jogait és a magánszféra védelméhez való jogát. A genetikai adat fogalma nemcsak a DNA vizsgálat eredményeként kapott adatokat, hanem a régebben alkalmazott módszerekkel (családtörténet, külsőleg megfigyelhető jelek elemzése stb.) megszerezhető adatokat is magában foglalja. A genetikai teszt feltárja a betegségekre való fogékonyságot és hajlamot. Ezek az információk döntő szerepet játszhatnak egy ember későbbi életében. A genetikai adatok – és általában a nagyon személyes vonatkozású egészségügyi adatokra is igaz – vonatkozásában nagyon fontos a következő három alapelv: *a)* az adatalanynak joga van *megismerni* az eredményt (right to know) *b)* az adatalanynak joga van *meg nem ismerni* az eredményt (right not to know) és *c)* joga van ahhoz, hogy *mások ne ismerhessék meg* az adatokat (the right not to have the others know)

A genetikai adatok szintén a felszínre hozzák magánszféra jogi vizsgálatánál léptennyomon meglévő alapvető dilemmát: miként lehet összeegyeztetni a munkavállaló, a munkáltató és köz érdekét.

A genetikai teszt esetén is fennáll az a tétel, hogy az érintett beleegyezése önmagában nem legitimálja a genetikai teszt elvégzését és a keletkező adatok feldolgozását.

A biomedicina jelenlegi állása szerint az esetek többségében a gének nem teljes mértékben határozzák meg az egyes betegségek előfordulását és fejlődését. A betegségek túlnyomó többségénél a kialakulás több faktorra vezethető vissza és a betegség tényleges bekövetkezése sem csupán a génektől függ, hanem a környezet és más tényezők kölcsönhatásától. A genetikai információk nem adnak teljes körű képet, különösen nem az egyéni munkavállaló szintjén.

A genetikai adatok magukban hordozzák a diszkrimináció lehetőségét, amely különösen jól érzékelhető a munkavégzés világában. Ezért feltétlenül figyelembe kell venni az EU Alapvető Jogok Kartáját (Charter of Fundamental Rights, 1989). A Karta 21. cikkelye kimondja, hogy mindennemű diszkrimináció tilos, beleértve a genetikai sajátosságokon alapuló hátrányos különbségtételt is.

A genetikai tesztek elvégzése sokba kerül. Ezért korábban sok munkáltató eleve lemondott a teszt elvégzéséről. Ugyanakkor a technológiai fejlődés eredményeként várható, hogy ezek a tesztek is olcsóbbak lesznek. Ezért a jövőben ezeknek a teszteknek várhatóan nagy piacuk lesz, ami további komoly felhasználói szabályozást igényel.

Másrészt azt is figyelembe kell venni, hogy a genetikai ellenőrzés és teszt eredményei hozzájárulnak a munkavállaló munkahelyi egészségének és biztonságának a növelé-

[35] I. m. pp.14–15.

séhez, különösen igaz ez olyan munkavállalók esetén, akiknek a munkaköre fokozottan veszélyes.

A genetikai tesztre vonatkozóan a következő alapelvek emelendők ki:

a) Jövőbe mutató genetikai adatok kezelésére és feldolgozására csak kivételes esetekben kerülhet sor. Kivételes esetnek minősül a munkavállaló vagy külső harmadik személy egészségének és biztonságának a megóvása, feltéve, ha a tagállami jogszabályok lehetővé teszik az adatgyűjtést és feldolgozást és a következő garanciális elemeket biztosítják:

b) Az arányossági elv (proportionality principle) következetes betartása: nem okozhat nagyobb hátrányt, mint ami az elérni kívánt cél megvalósítása érdekében feltétlenül szükséges.

c) A genetikai teszt eredményeinek a felhasználásán alapuló munkavégzési feltételek javítása nem eredményezhet előítéleteket.

d) A tesztet előzetes genetikai tanácsadásnak kell megelőznie.

e) Szükséges a nemzeti ellenőrzési hivatal (national supervisory authority) előzetes kontrollja.

f) Az előzetes ellenőrzés során minden egyes eset sajátos körülményeit figyelembe kell venni: *fa)* A teszt minőségét; *fb)* az eredmények relevanciáját és megbízhatóságát; *fc)* egyensúlyteremtés a következő elemek között: *a)* az érintett személy joga; *b)* a nyilvánvaló társadalmi érdekek; különösen a munkatársak vagy külső harmadik személyek egészsége és biztonsága, elsősorban az egészségre ártalmas munkakörök esetén; *c)* az információk visszatartásához való jog – nem közlik az érintett személlyel a tényleges állapotára vonatkozó adatokat –, gyógyíthatatlan betegségben szenvedő személyek esetén.[36]

2.8.11. A munkavállaló megfigyelése és ellenőrzése

A munkavállalók viselkedésének a megfigyelése és az (elektronikus) levelezésük ellenőrzése olyan kérdések, amelyek jelenleg a viták középpontjába kerültek.

Elöljáróban megjegyezzük, hogy a munkahelyen belül alapvetően kétfajta e-mail használatot különböztethetünk meg:

a) Az egyik, amikor csak az üzleti célú használat engedélyezett. Ilyenkor a munkáltató ellenőrzési joga ezekre az üzleti tartalmú dokumentumokra kiterjed.

b) A másik eset, a magáncélú használat. Ilyen esetben a munkáltató csak biztonsági céllal és akkor sem rendszeres ellenőrizheti a munkavállaló privát levelezését.[37]

A tagállamok különböző szintű jogi normája – alkotmány, munkajogi szabályozás, adatvédelmi szabályozás, telekommunikációs szabályozás, büntető törvénykönyv stb. –és alapelvei foglalkoznak a megfigyelés és ellenőrzés kérdéseivel. A különböző normák kölcsönhatása – legalábbis a munkavégzés terén – nem minden esetben problémamentes. Sok esetben a tényállások nem teljesen tiszták és a szituációk is ellentmondásosak.

Várhatóan a jogi helyzet a jövőben még tovább bonyolódik, miután az eddig használt tradicionális megfigyelési módszereket – pl. telefonos lehallgatás, videokamerás megfi-

[36] I. m. pp.15–16.

[37] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 5.

gyelés stb. – a rohamos technikai haladásnak megfelelően felváltja és/vagy kiegészíti egy sokkal hatékonyabb, a munkavállaló saját elektronikus munkaeszközén – e-mail, internet stb. – keresztül történő megfigyelés és ellenőrzés.

A munkavállalók megfigyelésére és ellenőrzésére vonatkozóan a következő elveket kellene az európai keretmegállapodásba belefoglalni:

a) A munkavállalók érdekképviseleti szervét informálni kell és konzultációt kell lefolytatni velük minden olyan munkahelyi rendszer bevezetése, módosítása, vagy a bevezetés előtt szükséges értékelése előtt, amelyet a munkavállalók megfigyelésére vagy ellenőrzésére használhatnak.

b) A tagállami Adatvédelmi Felügyeletet ellátó hatóság (National Data Protection Supervisory Authority) előzetes ellenőrzése.

c) Folyamatos megfigyelés csak kivételes esetekben engedélyezett. Ilyen lehet például, az egészségügyi, biztonsági vagy vagyonvédelmi célból szükséges megfigyelés.

d) Titkos megfigyelés csak a vonatkozó tagállami jogszabály rendelkezéseinek szigorú betartásával lehetséges, illetve akkor, ha bűncselekmény vagy egyéb súlyos kötelezettségszegés elkövetésének alapos gyanúja merül fel.

e) Az adott munkahely biztonságos működése, illetve az alkalmazott technológia használatának ellenőrzés során gyűjtött adatokat nem lehet általában a munkáltatónál dolgozó munkavállalók magatartásának az ellenőrzésére használni, kivéve azokat a munkavállalókat, akik a vizsgált eszközöket, technikát stb. működtetik.

f) Az elektronikus úton gyűjtött információk nem szolgálhatnak a munkavállaló munkaértékelésének kizárólagos alapjául, illetve a rá vonatkozó munkáltatói döntések meghozatalánál.

g) A biztonsági okból vagy a rendszer megfelelő működésének technikai ellenőrzése (pl. vírusos-e a rendszer stb.) miatt végzett beavatkozások esetén, tilos a minden egyes munkavállaló e-mail/Internet forgalmát rendszeresen ellenőrizni. Az egyéni megfigyelésre csak akkor kerülhet sor, ha bűncselekmény elkövetésének alapos gyanúja, vagy súlyos munkavállalói kötelezettségszegés, illetve súlyos magatartásbeli probléma merül fel és a munkáltató céljának az eléréséhez nem áll rendelkezésre az egyéni megfigyelésnél finomabb módszer vagy technika (Például csak az e-mail/Internet forgalmazás adatainak – objektív alapon történő – megfigyelése úgy, hogy a levelezés tartalmát nem vizsgálják.)

h) A munkáltató nem nyithatja meg a munkavállaló magán e-mail-jeit, illetve egyéb magáncélú file-kat, feltéve ha ezekből nyilvánvalóan kiderül, hogy magáncélúak. Ez a tilalom akkor is vonatkozik a munkáltatóra, ha a munkavállaló a munkáltató tulajdonában lévő eszközt használta. Sőt attól is független, hogy a munkáltató engedélyezte-e a magáncélú használatot vagy sem. A magánjellegű e-mailt úgy kell tekinteni, mint a postai magánlevelezést. A levelezés titkosságának jogáról a munkavállaló puszta hozzájárulásával – rendszerint a munkaszerződésben lévő klauzula aláírásával – nem mondhat le.

i) Speciális védelemben kell részesíteni a munkavállalónak a munkaegészségügyi szolgálattal és a munkavállalói érdekképviseletekkel folytatott kommunikációját.[38]

A kívánatos munkáltatói magatartás esszenciális elemei a megfigyeléskor:

[38] http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf; Second stage consultation of social partners on the protection of worker's personal data, p. 16–17.

A munkavállaló előzetes informálása a megfigyelés tényéről, céljáról és módszeréről;

Az elektronikus kommunikációs – e-mail/Internet – rendszer nem megengedett célra történő alkalmazása megalapozza a titkos megfigyelést vagy a már megkezdett megfigyelés folytatását. Alapesetben a titkos megfigyelés nem megengedett magatartás.[39]

3. Az EU Közösségi szintű szabályozására vonatkozó fontosabb megállapítások

A személyes adatok kezelésre vonatkozó szabályozás nem más, mint egy érzékeny kompromisszum sarkpontjainak a megtalálása. A munkaviszony keretében mindkét félnek (munkáltató-munkavállaló) megvannak a jogai és a jogos érdekei. Számos esetben a munkáltatónak joga, sőt bizonyos esetben kötelezettsége a munkavállalókra vonatkozó személyes adatok gyűjtése és feldolgozása. Például, bizonyos munkaviszony – tanár, bíró, szociális munkás stb. – létesítésekor a jogszabály ún. előzetes vizsgálatot kíván meg. E mögött nyilvánvalóan az a jól megfontolt érdek áll, hogy csak olyan személy tölthesse be az adott állást, aki minden feltételnek megfelel. Az EU álláspontja szerint a munkáltatóknak csak a jogszabályok által előírt – a munkavállalót érintő döntéshez minimálisan szükséges – információhoz szabad csak hozzájutniuk. Például, nem tekinthetnek bele a munkavállaló teljes egészségügyi dokumentációjába, hanem csak ahhoz az információhoz juthatnak hozzá, amely megmondja, hogy az illető személy alkalmas-e az adott munkakör betöltésére vagy sem. A Közösségi jogalkotás két elvet kíván követni: *a)* következetes tiltás és *b)* eseti ellenőrzés. A munkahelyi megfigyeléssel kapcsolatban szintén felmerül az egyensúly kérdése. Sok munkáltató hiszi azt, hogy mivel a saját tulajdonát képezi a számítógép ezért joga van arra, hogy szabadon megtekinthesse annak a tartalmát. A másik oldalon a munkavállaló áll, aki szerint ez a munkáltatói szabadság sérti az ő személyiségi jogait. A munkahelyi megfigyeléssel és ellenőrzéssel kapcsolatban a Közösség álláspontja, hogy a megfigyelést nyíltan kell végezni, amelyet bizonyos körülmények esetén lehet elvégezni és szükséges a szakszervezetekkel tárgyalni róla. A munkáltató tehát ne nézhessen bele a munkavállaló privát e-mail és Internet forgalmába, illetve ne nyithassa meg a számítógépen lévő magánjellegű adatállományait, még akkor sem, ha nem engedte meg a munkahelyen a munkáltatói elektronikai eszközök magáncélú használatát.[40]

Összefoglalva: a Bizottság kihangsúlyozza, hogy a munkavállalók személyes adatai csak előre konkrétan meghatározott célra (defined purpose) használható fel. Nem elég önmagában a szükségesség (necessity) és az arányosság (proportionality) elvének a betartása.

[39] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 4.

[40] Minimum standards for employee data privacy; Social Agenda, December 2002. p. 3–4.

II. rész
A munkavállalók elektronikus kommunikációjához kapcsolódó személyes adatok a védelme az EU tagállamok és az Európai Gazdasági Térség államainak a jogában

Bevezetés

Napjainkban az Európai Unió tagállamaiban is az e-mail és az Internet használat elválaszthatatlanul hozzátartozik a munkavégzők jelentős többségének a munkájához. Vitán felül áll, hogy a jövőben ez a trend tovább folytatódik. Az elektronikus levelezés nagyon sok előnyös vonása azt eredményezte, hogy ma az e-mail az üzleti élet – mind a cégen belüli, mind pedig a cégek közötti – egyik leginkább használt kommunikációs eszköze.

Az e-mail legfontosabb előnyei: olcsó, gyors, kényelmes, nagy terjedelmű dokumentumot bármilyen nagy távolságra is alacsony áron lehet továbbítani, a folyamatosan bekapcsolt terminálok eredményeként a felek szinte állandó kapcsolatban állnak egymással, úgy hogy közben végezhetik a saját munkájukat. Mindössze egy hangjel a számítógépből jelzi, hogy új levél érkezett. A címzett pedig szinte azonnal képes reagálni az érkezett levélre. Sőt, néhány perc elteltével a küldő meg is kaphatja a választ. Akár interaktív „beszélgetést" is folytathatnak. Ennek eredményeként az ügyek a lehető leggyorsabban és remélhetőleg mindkét fél megelégedésére zárulhatnak.

Miután az üzleti világban nagyon gyorsan felfedezték az e-mail és az Internet előnyeit, napjainkban már kezdenek foglalkozni ezen kommunikációs csatornák hátrányos vonásaival is. A leggyakrabban említett problémák a következők: nem megfelelő használat esetén az adott cég reputációján csorba eshet, üzleti titkok kerülhet ki a cégtől, rágalmazások csatornája lehet, a munkáltatói tulajdon megengedett vagy meg nem engedett használatának a kérdése, használatukkal a munkavállalók munkaidőben végezhetik a magánjellegű dolgaikat, a munkahelyi zaklatás eszközei lehetnek, vagy segítségükkel bárkihez pornográf jellegű anyagokat lehet eljuttatni, stb. A fenti hátrányokat alapvetően a következőképpen foglalhatjuk össze: a munkáltató tulajdonában álló eszközök és az általa alkalmazott elektronikus rendszer jog- illetve normaellenes és/vagy a munkáltató gazdasági érdekeivel ellentétes alkalmazása a munkavállaló(k) által.

Napjainkban még – a fejlett ipari társadalmakban is – ténykérdés, hogy az internetes kérdéseket szabályozó normaalkotás jóval a technikai fejlődés mögött jár.

Általánosságban megállapítható, hogy az egyes – megközelítőleg azonos gazdasági fejlettségű – országokban a munkahelyi e-mail és Internet használat sajátosságai alapvetően megegyeznek. A munkahelyi Internet és e-mail használattal kapcsolatban a munkaviszony két alanyának – munkáltató és a munkavállaló – fontos, egymással sokszor ellentétes érdekei és megközelítési módjai kerülnek egymással szembe. Ez a két ellentétes érdek a következő. A munkáltató oldalán az a jog, hogy jogszerűen megfigyelhesse és kontrolálhassa a munkavállalói tevékenységet. A munkavállalók oldalán pedig a magánszférához, a személyiségi jogaik védelméhez való jog. A legtöbb államban az alkotmány, a személyiségi jogokról rendelkező normák, az adatvédelmi törvény és a telekommunikációs jogszabályok foglalkoznak ezzel a problémával.

Az is megállapítható, hogy mára a legtöbb fejlett országban található olyan jogi szabályozás, amely a személyiségi jogokkal vagy a magánszféra védelmével foglalkozik.

Ugyanakkor némely országban a magánszférát védő jogi normák és a munkáltatók ezzel ellentétes gazdasági érdekeit védő normák egymással „kiegyenlítődnek". Például Ausztriában a munkáltató megtilthatja a munkavállalóinak a munkahelyi e-mail és Internet privát célú alkalmazását. Ezt követően – egy esetleges jogvita esetén - a munkavállaló már nem hivatkozhat arra, hogy a küldött e-mail magán természetű volt. Ilyen esetben a munkáltató jogszerűen jár el, ha a munkavállaló által küldött minden egyes e-mail-t ellenőrzi, illetve a munkáltató minden egyes e-mail-t úgy tekint, mintha azok kivétel nélkül üzleti jellegűek lennének, tehát általa megtekinthető.

Más államokban nincs ilyen kiegyenlítő mechanizmus, hanem a természetes személy magánszférájának a védelme kiemelt szerepet kap. Például Franciaországban, a Legfelsőbb Bíróság Szociális Kollégiuma 2001 októberében a „NIKON France" ügyben hozott ítéletében a következőket mondta ki: „a munkavállalók joga a magánszféra és a személyiségi jogok védelmére olyan elidegeníthetetlen és alapvető emberi jog, amelyet a munkáltató semmilyen magatartásával nem sérthet meg. A konkrét ügy kapcsán a bíróság kimondta, hogy a munkáltató alapvetően nem ellenőrizheti a munkavállalók munkahelyi e-mail-jeit, még abban az esetben sem, ha a munkáltató világosan megtiltotta a munkavállalóknak a munkahelyi információs rendszer magáncélú használatát."

Az adatvédelem jogi szabályozása is országonként jelentős eltérést mutat. Néhány országban a szabályozás nagyon kifinomult és külön cikkelyek vonatkoznak az e-mail és az Internet használatra. (pl. Svájcban a szövetségi Adatvédelmi Biztos kibocsátott egy ajánlást, amely az email és Internet munkahelyi használatának a megfigyeléséről szól.) Németországban az adatvédelemre vonatkozó normák nem biztosítanak speciális előírásokat, hanem ilyen esetben is a személyiségi jogok védelmére vonatkozó általános szabályok alapján lehet eljárni. Hollandiában nincs külön adatvédelmi törvény, hanem a magánszféra védelméről rendelkező törvény (Wet Bescherming Persoonsgegevens – Privacy Act) foglalja magában az adatvédelemre vonatkozó jogokat és kötelezettségeket. A fentiekből következően nem meglepő, hogy Európán belüli államokban is jelentős eltéréseket mutató szabályozással találkozunk. Így például Svájcnak és Nagy Britanniának eltérő filozófián alapuló jogi szabályozása van.

Általában a telekommunikációs joganyag hatálya alá tartozik az e-mail és az Internet használatának a szabályozása is. Például, Belgiumban a Belgacom Statute vagy Németországban a Teleservice Data Protection Act (TKG), illetve a Data Protection Act (TDDSG) rendelkezik erről a kérdésről.

Az európai joggyakorlatban a magánszféra védelmét illetően az Európai Emberi Jogi Bíróság Halford v. The United Kingdom ítélete (1999) meghatározó jelentőségű. Az eset kapcsán a bíróság elsősorban a telefonbeszélgetés lehallgatásával kapcsolatban foglalt állást. Ez közvetett módon érinti mind az e-mail, mind pedig az Internet forgalmat.

A vonatkozó jogszabályok jelenleg nem írják elő a munkavállalói érdekképviselettel vagy az Európai Üzemi Tanáccsal való előzetes konzultációt az e-mail vagy Internet magáncélú használata, illetve a privát használat esetére előírható szankciók vonatkozásában. Ugyanakkor a szociális partnerekkel történő konzultáció – kisebb, vagy nagyobb mértékben – kötelező Ausztriában, Belgiumban, Franciaországban, Hollandiában és Németországban.

További súlyos problémaként jelentkezik a bizonyítás kérdése. A magáncélú e-mail/Internet használat esetére megállapítható szankció kiszabásának egyik fontos előfeltétele az elkövetett normasértés (jogellenesség) és az okozati összefüggés bizonyítása.

Ez a bizonyítási teher a munkáltatón van. Ugyanakkor a munkáltatónak nagyon limitált lehetősége van arra, hogy beszerezze a szükséges bizonyítékokat. A bizonyítékokat csak nagyon óvatosan lehet összegyűjteni. Például Németországban, ha a munkáltató a bizonyítékok beszerzése során túllépi az engedélyezett határt, akkor az így szerzett bizonyíték nem szolgálhat a munkaviszony megszüntetésének okaként.

A vizsgált országokban egyértelműen az az álláspont alakult ki, hogy a munkáltatónak célszerű egy a munkahelyi e-mail és Internet használatáról rendelkező írásbeli szabályzat megalkotása. Ez a szabályzat közvetlen kapcsolatban áll a munkáltató fegyelmi eljárási rendjével. Következésképpen a munkavállalónak tudnia kell, hogy a szabályzatban foglaltak megsértése fegyelmi eljárást von maga után, ami végső soron a jogviszony megszüntetését eredményezheti.

A következőkben az egyes – kiemelt – tagállamok bemutatásánál a következő kérdéseket vizsgáljuk: *a) A munkáltató ellenőrzési joga*: vajon joga van-e és ha igen akkor milyen mértékben és milyen jogalapon a munkavállaló munkahelyi e-mail és Internet forgalmának ellenőrzésére; *b) Szankciók és felelősségi kérdések*; és *c) Az ellenőrzés technikai mikéntje*: milyen konkrét módszerek segítségével tud különbséget tenni a munkáltató a magán és a hivatali célú Internet vagy e-mail használat között.[41]

Ausztria

1. A munkáltató ellenőrzési joga

Napjainkban Ausztriában is a munkavégzés során az e-mail és az Internet használata majdnem olyan gyakori, mint a telefoné. Éppen ezért teljesen magától értetődik, hogy a munkáltatóknak értékelni kell a helyzetet és el kell gondolkodniuk azon, hogy milyen módon védekezhetnek ezen munkahelyi eszközök illegális használata ellen.

Jelenleg az osztrák munkajog nem tartalmaz olyan konkrét szabályokat, amelyek az e-mail, illetve az Internet munkahelyi ellenőrzéséről rendelkeznének. Sőt, még a bírói gyakorlatban is csak nagyon kevés ilyen eset fordult elő. Ugyanakkor, kialakult az a nézet, hogy a munkahelyi e-mail és Internet magáncélú használatának a kérdése a munkajogi alapelvek és munkahelyi telefonbeszélgetésekre vonatkozó bírói gyakorlat segítségével megoldható.

A munkáltató ellenőrzési joga minden munkaviszonynak az esszenciális része. A munkáltatónak ez a joga a vonatkozó munkajogi normákon és a munkaszerződésen alapszik. A munkahelyi e-mail és Internet használat ellenőrzésének másik jogi alapja a tulajdonjogból vezethető le: a munkáltató a tulajdonosa annak a hardvernek és szoftvernek, amellyel a munkavállaló dolgozik. A munkáltató tulajdonjoga lehetővé teszi, hogy ellenőrizze a tulajdonát képező eszköz használatát. (Sec. 354 of the Civil Code – Allgemeines Bürgerliches Gesetzbuch – AGBG)

A munkáltató ellenőrzési joga azonban nem korlátlan. Számos jogszabályhely ír elő korlátozást. Az első a AGBG 16. cikkelye, amely a munkavállaló személyének az integritását hivatott védeni. További rendelkezés, amely Ausztriában a személyiségi jogokat, mint alapvető emberi jogot védi (Art. 8 European Human Rights Convention), illet-

[41] http://www.cmslegal.com/intelligence/cms_news/email_Internet.htm: The use of email and the Internet in the workplace in Europe.

ve a levéltitok és telekommunikációs beszélgetések sérthetetlenségét előíró szabályozás [Art. 10 és 10/a Charter of Fundamental Rights – Staatsgrundgesetz – STGG(1867)] A fenti nemzetközi normákban szereplő alapvető emberi jogokat az osztrák alkotmány is garantálja.

Az adatvédelmi törvény (Datenschutzgesetz – DSG; 2000) – alkotmányból kapott felhatalmazás alapján – kimondja, hogy minden személynek joga van ahhoz, hogy a személyes adatai védelemben részesüljenek.[42] A törvény korlátozza a személyes adatok felhasználását és ellenőrzését. A személyes adatokat a munkáltató két esetben használhatja fel jogszerűen: a) a munkavállaló beleegyezik vagy b) a munkáltató gazdasági érdeke indokolja. További feltétel, hogy a munkáltató minden esetben köteles informálni a munkavállalóját, ha a személyes adatait fel kívánja használni (Sec. 24 DSG).

Bizonyos körülmények fennállta esetén a Telekommunikációról rendelkező törvény (Telekummunikationsgesetz – TKG, 1997) ugyancsak korlátozza a munkáltató ellenőrzési jogát. A törvény előírja a telekommunikációs szolgáltatást nyújtó személynek (szervnek), hogy köteles a felhasználó bizonyos adatait titokban tartani, továbbá köteles megakadályozni a telefonvonalak lehallgatását és arról sem szolgáltathat ki adatot, hogy a felhasználó mikor és kivel folytatott elektronikus kommunikációt. (Sec. 88 TKG) A szabályozás szépséghibája, hogy a nagyobb munkáltatóknak saját web szolgáltatójuk van, tehát a fenti megszorítás rájuk nézve nem alkalmazható. Ugyanakkor a kis és közepes munkáltatók rendszerint valamely külső Internet szolgáltató céggel kötnek szolgáltatási szerződést. A törvény fent ismertetett rendelkezése rájuk nézve mérvadó. Mivel a kis és közepes nagyságú munkáltatók külső szolgáltatókkal szerződve jutnak a szolgáltatáshoz, számukra nehéz feladat a munkavállalók által használt e-mail és Internet direkt ellenőrzése.

A munkáltató ellenőrzési jogának további korlátozását a Kollektív szabályzásról rendelkező törvény [Sec. 96 par. 1. num. 3 of the Collective Regulatory Act (Arbeitsverfassungsgesetz – ArbVG)] és az Individuális Munkajog Adaptációjáról rendelkező törvény [Sec. 10 of the Individual Labour Law Adaptation Act (Arbeitsvertragsrechts–Anpassungsgesetz AVRAG)] jelenti. Mindkét jogszabályhely az ellenőrzés technikai módszereire utalva korlátozza az olyan megfigyelést, amely a munkavállalók emberi méltóságát sérti vagy sértheti. Az ilyen jellegű – a törvény által korlátozott megoldások – csak abban az esetben lesznek jogszerűen alkalmazhatók, ha abba az érintett munkavállaló vagy az üzemi tanács határozott beleegyezését adta.

További kérdésként merül fel, hogy az osztrák jogszabályok lehetővé teszik-e a munkáltatónak, hogy megtiltsa a munkavállalónak a munkahelyi e-mail és Internet privát célú használatát. Mivel a kérdésben még nincs esetjog Ausztriában, leginkább a jogirodalomhoz tudunk segítségért folyamodni.

E kérdés tárgyalásánál emlékeznünk kell arra a fontos tényre, hogy az eszközök, amelyen keresztül a kommunikáció folyik (hardware és software) egyaránt a munkáltató tulajdona. Ezért több szerző arra az álláspontra helyezkedik, hogy a tulajdonhoz fűződő jogok közül a rendelkezési jogból következik, hogy a munkáltató jogszerűen megtilthatja a munkavállalóknak a magáncélú (jogszerűtlen) használatot. A Legfelső Közigazgatási Bíróság (Supreme Administrative Court) egy a telefonhívások rögzítésére alkalmas számítógéppel (amely rögzíti a hívott számot, a hívott felet, a hívás tartamát és költsé-

[42] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 32.

gét) kapcsolatos ügyben arra az álláspontra helyezkedett, hogy a munkáltatónak joga van ahhoz, hogy megnézze (ellenőrizze) ki, mikor és meddig használta a telefonvonalat.[43] Ezt az álláspontot az osztrák Legfelsőbb Bíróság (Oberster Gerichtshof) is osztotta.[44] Azért kell analógiát alkalmaznunk, mert a bírói gyakorlatban elsősorban még a hagyományos telekommunikációs eszközök – pl. telefon – használatával kapcsolatban születtek döntések.

Más lesz a döntés megközelítése (jogalapja) az ún. vészhelyzetben történő (sürgősségi) telefonhasználat esetén. Ilyenkor magától értetődik, hogy a munkavállaló a különösen indokolt, a személyét vagy munkatársát vagy esetleg más külső harmadik személy testi épségét érintő vészhelyzetben vagy a munkáltató érdekeit veszélyeztető magatartás következményeinek az elhárítására használhatja a munkáltató telefonját, vagy e-mail-jét.

Ha a munkáltatónak joga van arra, hogy csak üzleti célra korlátozhatja az e-mail vagy Internet használatot, akkor arra is fel kell jogosítani, hogy ellenőrizhesse, hogy a munkavállalók betartják-e az utasítását vagy sem. Amikor a munkáltató gyakorolja ezt a jogát, akkor minden esetben köteles szem előtt tartani a munkavállalók magánszféráját védő általános szabályokat és a rá vonatkozó speciális előírásokat.

Ausztriában a munkáltatói ellenőrzési jogosultsága sok tényezőtől függ. Először is attól, hogy a munkavállaló jogszerűen használhatja-e a munkahelyi email-t magán célra vagy sem. Amennyiben csak hivatali célra használhatja az e-mail-t, akkor a munkáltató szabadon ellenőrizheti azt, hiszen a munkavállaló nem hivatkozhat arra, hogy bizalmas információkat is forgalmazott. Ilyen esetben a munkahelyi e-mail jogi megítélése megegyezik a céges papíron és borítékban küldött postai levél statusával. A munkáltató ilyenkor szabadon ellenőrizheti a munkavállalója által küldött e-mail-t, csakúgy mint azt a céges papíron írt levéllel teheti. Ugyanez a logika vonatkozik az Internet használatra is.

Abban az esetben, ha a munkáltató nemcsak a kimenő, hanem a bejövő (válasz) leveleket is szeretné megvizsgálni, akkor változik a jogi helyzet, hiszen ilyenkor már egy külső harmadik személy is részt vesz a levelezésben. Ilyen esetben az a leggyakoribb megoldás, hogy a kimenő levelek alján jelzik a címzettnek, hogy az erről a munkahelyi címről küldött elektronikus levelek nem tekinthetők bizalmas levélnek, hanem azokat a levelezésben lévő személyeken kívül mások is elolvashatják.

Más a jogi megítélése annak, amikor a munkáltató nem tiltja meg kifejezetten a munkahelyen a privát célú levelezést, vagy amikor azt kifejezetten jóváhagyja. Abban az esetben, ha ezeknél a munkáltatóknál nem működik üzemi tanács, akkor a munkavállaló egyedüli védelmét a magánszféra védelmére vonatkozó jogszabályok és a levéltitok védelmére vonatkozó szabályok képezik. A munkavállaló erről a jogáról lemondhat. Ugyanakkor a munkaszerződésből következően a munkáltatót megilleti az ellenőrzéshez való jog, hiszen meg kell győződnie arról, hogy a munkavállaló betartja-e a munkáltató által alkotott szabályzatban (code of conduct) írottakat. Ilyen esetben a feleknek rögzíteniük kell az ellenőrzés módját, eszközeit stb.

[43] Verwaltungsgerichtshof 11.111987, ARD 33951/11/88.
[44] 21.10.1988, RdW 1999, 425.

Ha a munkahelyi e-mail és Internet forgalom ellenőrzésére szolgáló kontroll eszköz sért(het)i a munkavállaló emberi méltóságát,[45] akkor ilyen berendezés vagy módszer csak az üzemi tanács beleegyezésével alkalmazható (Sec. 96 num. 3 ArbVG).

A most tárgyalt jogesetben a munkáltató egy olyan számítógépes szerkezetet építetett be az e-mail és az Internet forgalmazás rendszerébe, amely segítségével kontrolálni tudta a beszélgetési időtartamát, díját és a hívott számot.[46] Magáncélú telefonhívás esetén a munkavállaló egy gomb lenyomásával ki tudja iktatni ezt az ellenőrző rendszert. A Legfelsőbb Közigazgatási Bíróság arra az álláspontra helyezkedett, hogy ez a módszer nem érinti hátrányosan a munkavállaló emberi méltóságát. Ilyenkor nem kell az üzemi tanács előzetes hozzájárulása az ellenőrző rendszer beszereléséhez és működtetéséhez.

A Legfelsőbb Bíróság ítéletének a tükrében kijelenthető, hogy a munkáltató minden munkahelyi elektronikus forgalmazás – pl. a munkavállaló által meglátogatott internetes honlapok címeinek stb. – ellenőrzése esetén köteles kikérni az üzemi tanács hozzájárulását. Miután az üzemi tanács nem gyakorolhatja ezt a jogát olyan esetben, amikor a munkavállaló individuális jogait érintené a döntés – pl. a telekommunikációs forgalmazáshoz való titok (Sec. 88 TKG) –akkor a munkáltatónak minden egyes érintett munkavállalótól meg kell kérni a beleegyezését.

A munkáltató munkavállalókra lebontva ugyancsak szabadon ellenőrizheti a munkahelyi email vagy Internet használat – egy munkavállalóra eső – költségét. Ilyenkor nem kerül sor tartalmi ellenőrzésre, csak az egyénre vetített költséget vizsgálja a munkáltató.

2. Szankciók

Teljesen magától értetődik, hogy egy munkavállalóval szemben csak akkor szabható ki szankció, ha bizonyítható, hogy felelős valamely jogellenes magatartásért. Ez lehet a munkaszerződésben foglaltak megszegése, vagy polgári, illetve büntetőjogilag értékelhető munkavállalói magatartás. A munkahelyi viselkedési kódex is számtalan munkajogi (fegyelmi) szankciót tartalmaz. A kiszabható szankcióknak széles tárháza található. Kezdve az egyszerű figyelmeztetéstől a munkaviszony azonnali hatályú megszüntetéséig. Egyetlen munkahelyi szabályzatban szereplő szankció sem vezethető be az üzemi tanács beleegyezése nélkül.

A munkavállaló minden olyan magatartásáért felelős, amellyel – az e-mail/internet jogellenes használat során – a munkáltatójának kárt okozott. A munkavállaló munkajogi felelőssége az osztrák jogban is limitált és munkavállaló-barát. Következésképpen a munkavállaló csak a jövedelmének egy meghatározott havi összegéig lesz felelős, tehát amennyiben a kár összege ezt a limitet meghaladja, akkor a teljes okozott kárt nem kell megtérítenie a munkavállalónak.

3. Az e-mail és Internet használata

Határozott álláspontnak tekinthető Ausztriában, hogy a munkáltató akkor jár el helyesen és preventív módon, ha megalkotja a vállalati e-mail/Internet szabályzatot. A szabályzat legfontosabb szerepe, hogy megtanítsa a munkavállalókat a helyes és biztonságos e-mail

[45] Az emberi méltóság tartalmilag a személyt megilleto emberi jogként határozható meg (pl. a magánszféra védelméhez való jog és a levéltitokhoz való jog).

[46] Administrative Supreme Court 11.11.1987, ARD 33951/11/88.

és internet használatra, valamint az elektronikus kommunikációra vonatkozó világos és egyértelmű szabályokat tartalmazzon. A szabályzatnak legalább a következő pontokat kell(ene) tartalmaznia:

a) a munkavállaló jogát az e-mail/Internet eléréshez;
b) a felhasználói titkos kód elárulásának a tilalmát;
c) bármely software (program) letöltésének és elküldésének a tilalmát;
d) a munkavállalói e-mail/Internet használat szabályait;
e) a pornográf és radikális politikai honlapokra történő belépés tilalmát;
f) a munkavállaló csak addig használja az internetet, amíg arra a munkájához szükséges (pl. megszerezte a releváns információt stb.), majd haladéktalanul ki kell lépnie onnan;
g) a jogsértő magatartás esetén megállapítható szankciók körét.

A szabályzat megalkotását a munkáltató egyoldalú döntése vagy kollektív szerződés, vagy a munkaszerződés előírásai rendelhetik el.

Amikor a munkáltató engedélyezi a munkahelyen az e-mail/Internet privát célú alkalmazását, akkor intézkednie kell arról is, hogy a magánjellegű és az üzleti kommunikáció határozottan elkülönüljön. Az egyik módszer erre, amikor minden munkavállaló két e-mail címet kap. Az egyiket üzleti, míg a másikat magán célra használhatja. Ilyen esetben a munkáltat kötelessége, hogy egyértelműen jelölje a privát leveleket a küldött e-mail referencia részében.

A munkáltatónak az üzemi tanáccsal kell tárgyalni, ha egy olyan elektronikus kommunikációs kontrol rendszert kíván bevezetni, amely érinti a munkavállalók emberi méltóságát (Sec. 96 num. 3 ArbVG). Amennyiben ez a konzultáció elmarad, akkor bármely munkavállaló keresete nyújthat be a munkáltatójával szemben.

Az üzemi tanáccsal akkor is konzultálni kell, ha a bevezetendő rendszer nem érinti a munkavállalók magánszféráját és/vagy emberi méltóságát. Ennek az a magyarázata, hogy a hardware és a software munkavégzési eszköznek minősül, következésképpen az üzemi tanács javasolhatja, hogy a munkáltató kössön egy üzemi megállapodást (works agreement), amelyben ezen eszközök megfelelő használatát rögzíti (Sec. 97. par. 1 num. 6 ArbVG). Amennyiben a munkáltató nem kíván ilyen megállapodást kötni, az üzemi tanács a Munkaügyi Bíróság mellett működő speciális egyeztetési bizottsághoz (conciliation board) fordulhat. A bizottság a felek közötti érdekvitában kötelező érvényű döntést hoz.

Belgium

1. A munkáltató ellenőrzési joga

Alapvetően a következő főbb motivációk húzódnak meg a munkáltató azon törekvése mögött, hogy ellenőrizni szeretné a munkahelyi elektronikus forgalmat: *a)* a munkavállaló magatartása befolyásolhatja a munkáltató felelősségének fokát; *b)* a munkavállalók munkateljesítményének az ellenőrzése; *c)* a munkáltató kötelessége, hogy biztosítsa a munkavégzés anyagi és erkölcsi feltételeit.

Miután a munkaviszony egyik elvitathatatlan sajátossága az alárendeltségi viszony. Ebből a munkáltatónak két fontos jogosultsága ered:[47] *a)* utasítási jog (a munkavégzéshez kapcsolódó utasításokat adhat a munkavállalónak) és *b)* ellenőrzési jog (meggyőződhet arról, hogy a munkavállaló eleget tett-e a munkáltatói utasításnak).

Általánosan elfogadott alapelv, hogy függetlenül a munkáltatónál lévő szabályzatok előírásaitól, a munkaviszony alanyainak kölcsönösen tisztelniük kell egymást (együttműködési kötelezettség és rendeltetésszerű joggyakorlás elve). Ezen az alapelv végrehajtása során előfordulhatnak olyan esetek, amikor a munkáltató jogszerűen korlátozhatja a munkavállaló szabadságjogait, ezen belül is az e-mail/internet használatot.[48]

A bevezető gondolatokhoz tartozik még annak a tisztázása, hogy egyértelműen a munkáltató a tulajdonosa azoknak az eszközöknek, amelyek segítségével a munkavállaló használhatja az e-mailt/internetet. A tulajdonosnak pedig joga van a saját tulajdonát képező eszközök használatát ellenőrizni.[49]

1.2. Az alkalmazási határok

Az e-mail/Internet magáncélú használatának teljes körű tiltása vitatott. Akik megkérdőjelezik, azzal érvelnek, hogy ez nem más, mint a szólásszabadság korlátozása, amely alapvető emberi jog és amelyet több jogszabállyal egyetemben a Belga Alkotmány is deklarálja. Ugyanakkor az is igaz, hogy némely belső, munkahelyi szabályzat kifejezetten tiltja a magáncélú e-mail/Internet használatot. Ennek az álláspontnak a képviselői az egyszerű Internet használatának a megtiltását azért tartják jogszerűnek, mert felfogásuk szerint ez – a szó szoros értelmében – nem minősül kommunikációnak, hanem csak az információ szerzés egyik csatornájának tekinthető. Következésképpen a felhasználás megtiltása nem tekinthető a szólásszabadság korlátozásának.

Az igazi jogi problémát elsősorban nem az e-mail/Internet használat szabályozásának a megalkotása jelenti, hanem az, hogy a megalkotott szabályok betartását milyen formában lehet effektíven ellenőrizni. Amennyiben a munkáltató meg nem engedett eszközökkel ellenőrzi a szabályok betartását, akkor a legrosszabb esetben még büntetőjogi felelősségre vonásra is számíthat.

A kérdés szabályozásának legalább a következő kritériumoknak kell megfelelniük: *a)* magánszféra védelme; *b)* telekommunikációs jogszabályokkal kompatíbilis normaalkotás és *c)* a szabályoknak – az adott munkáltatón belül – minden egyes munkavállalói jogviszonyra alkalmazhatónak kell lennie. Ha ezek a feltételek egyidejűleg teljesülnek, akkor valószínűsíthető, hogy egy jó munkahelyi szabályzatot alkottak. A következőkben ezeket a kritériumokat tárgyaljuk.

1.3. Magánszféra védelme (privacy)

A belga Alkotmány 22. cikkelye garantálja a magánszféra védelméhez való jogot.

Az Emberi Jogok Európai Bíróságának a Niemietz ügyben hozott döntése óta általánosan elfogadott az az álláspont, hogy a munkavállalókat megilleti a magánszféra védelméhez való jog. A döntés az Emberi Jogok Európai Egyezségokmányának 8 cikke-

[47] Statute of the employment contracts 2, 3 és 172. cikkelyek.
[48] Statute of the employment contracts 16. cikkely.
[49] Polgári Törvénykönyv 544. cikkely és a Statute of the employment contracts 17.5. cikkely.

lyén, illetve a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának 17. cikkelyén alapul. Az Emberi Jogok Európai Egyezségokmánya és a belga alkotmány szerint a magánszférába történő minden beavatkozást jogszabályokban előre kell jelezni. A jogtudósok és a bírói gyakorlat egyöntetű álláspontja, hogy a jogszabályt nem megszorítóan, hanem tágan kell értelmezni. A munkahelyen belül létező és alkalmazott minden szabályt ide kell sorolni. Amennyiben a munkáltató be kíván avatkozni a munkavállaló magánszférájába, akkor az csak jogszerű okból történhet. Ilyen jogos ok lehet például a munkatársak jogának, illetve érdekének a védelme. A munkáltatónak szintén be kell tartani az arányosság elvét, vagyis a magánszféra megsértése mögött valamilyen társadalmilag indokolható oknak kell állnia. Nem elég, ha a munkáltatónak ez a beavatkozás hasznos, illetve kívánatos (gazdasági ok).

A fentiekből következik, hogy a munkavállalónak – elvileg – joga van a munkahelyi e-mail/Internet magáncélú használatához és a munkáltató csak egy nagyon szűk körben és szigorúan meghatározott feltételek mellett ellenőrizheti a munkavállaló ilyen tevékenységét.

A Belga Adatvédelmi Hatóság a 10/2000. számú Véleményében (Opinion no. 10/2000 of 3 April 2000) ugyancsak foglalkozott az e-mail/Internet megfigyeléssel. Ebben kimondták, hogy a munkáltatónak nincs joga megtekinteni a munkavállaló e-mail/Internet forgalmazását. Ilyenkor nem alkalmazható az arányosság elve. Az e-mail/Internet munkáltatói megfigyelése és kifürkészése nem indokolható semmilyen fontos munkáltatói érdekkel. A Hivatal azt ajánlotta a munkáltatóknak, hogy a levelezés tartalmi megtekintése helyett olyan technikai fejlesztéseket hajtsanak végre, amely segít az illegálisnak vélt levelezés vagy Internet használat csökkentésében. Például alkalmazzanak olyan programot, amely képes kiszűrni a bizonyos határon túl terjedő leveleket, vagy egy idő után nem engedi továbbítani a láncszerű levelezési forgalmat, vagy bizonyos internetes oldalakat nem enged megnyitni stb.

A hatóság ugyancsak állást foglalt a munkavállalói e-mail/Internet forgalom folyamatos megfigyeléséről. Állásfoglalásának az esszenciális magja úgy összegezhető, hogy a munkavállaló e-mail/Internet forgalmának a folyamatos megfigyelése alapvetően tilos. A hatóság azt javasolta a munkáltatóknak, hogy a munkavállalók konkrét azonosítása nélkül nézzék meg, hogy a munkavállalók milyen honlapokat látogattak. Ezt követően ki kell értékelni, hogy a meglátogatott oldalak közül melyik okozhat veszélyt a munkáltatóra, majd ezt követően kerülhet sor – az inkriminált oldalak használóival szemben – egyéni felelősségre vonásra.[50]

1.4. A telekommunikációra vonatkozó szabályozás

A Belgacom Statute 109 cikkely D. pontja és a Büntető törvénykönyv 314. cikkelye korlátozza a munkáltatónak a munkahelyi telekommunikációs eszközökre vonatkozó ellenőrzési jogát.

A Belgacom Statute különböző tiltásokat tartalmaz. Ezek közül egy lehet alkalmas a munkahelyi e-mail/internet használat szabályozására. Ez a jogszabályhely kimondja, hogy a munkáltató a munkavállaló vagy külső harmadik személy kifejezett beleegyezése hiányában nem használhat fel semmilyen – a munkavállalót vagy harmadik személyt

[50] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 27.

érintő – információt. A külső harmadik személynek akkor kell ilyen beleegyező nyilatkozatot adni, amikor a munkáltató az e-mail forgalmat ellenőrzi. Technikailag ez a beleegyező nyilatkozat úgy néz ki, hogy a munkáltató minden egyes küldött e-mail aljára odaírja, hogy a levél üzleti levélnek minősül, következésképpen a munkáltató által bármikor és bármelyik részében ellenőrizhető. Amennyiben a külső harmadik személy ezzel nem ért egyet, akkor ő maga köteles értesíteni a kifogásáról a munkáltatót.

A Belgacom Statute-ben szereplő tiltás magára a kommunikációs folyamatra, míg a Büntető törvénykönyvben szereplő szankció a kommunikáció tartalmára irányul. A Büntető törvénykönyv 314. cikkelye megtiltja a magánjellegű *kommunikáció küldésekor* a véletlen belehallgatást, abból való adatgyűjtést és annak a rögzítését. Kivétel, ha a felek előzőleg egyetértettek az ilyen munkáltatói magatartással. Ez a szabály mind az e-mail, mind pedig az internetes kommunikációra érvényes. Ki kell emelni, hogy ez a tiltás csak a küldés időszakára (küldés és fogadás) vonatkozik. A küldési folyamatot követően a tiltás már nem érvényes. Például, ha a munkavállaló kinyomtatja az e-mail szövegét és az asztalán hagyja a „kommunikáció" már nem védett. A tiltás arra az időszakra sem érvényes, amikor a munkáltató a rendszer működőképességét ellenőrzi vagy karbantartást végez és e miatt néz bele a levélbe. De ez a betekintés csak technikai okból és nem a tartalom kifürkészésére irányulhat.

1.5. Általános szabályok

Amennyiben nincs más megállapodás a munkahelyi e-mail/Internet használatára a munkáltató és a munkavállaló között, akkor ezen kommunikációs eszközök használatának szabályait a kollektív szerződésben, üzemi megállapodásban és más olyan munkahelyi szabályzatban – amelyet minden munkavállaló ismer (pl. munkahelyi szabályzat, viselkedési kódex stb.) – lehet rögzíteni. Arra vonatkozóan nincs konszenzus, hogy a munkaszerződésben lehet-e ilyen jellegű kérdéseket szabályozni.

Az e-mail/Internet használat ellenőrzésének a Polgári Törvénykönyvben szabályozott (1134. cikkely) általános érvényű alapelv – a szerződés végrehajtása során a feleknek jóhiszeműen kell együttműködniük, valamint a Statute on Employment Contract (16. cikkely), amely kimondja, hogy a munkaszerződés mindkét alanyának kölcsönösen tisztelni kell a másik felet – is korlátot szab. A fenti alapelvi szintű rendelkezésekből kiolvasható, hogy a munkáltató az ellenőrzés jogát csak egy megengedett tisztességes határon belül gyakorolhatja. Minden ezen felüli, meg nem engedett magatartás tilos.

A gyakorlatban az e-mail/Internet szabályozására analógiaként használják a levéltitokra vonatkozó szabályok egy részét. Meg kell jegyezni, hogy az alkotmány a levéltitok védelméről rendelkező cikkelye megszorító jellegű és csak a postai úton küldött levelet részesíti védelemben.

Végezetül létezik még néhány olyan norma, amely a titkos adatvédelemre vonatkozik (pl. minden a személyre vonatkozó információ[51]).

2. Szankciók

A munkáltató alapvetően két szankció közül választhat: a) munkaviszony rendkívüli felmondással történő megszüntetése és b) valamilyen egyéb szankció alkalmazása a

[51] Statute of 8 December 1992.

munkavállalóval szemben. Ha az első megoldást választja, akkor a tudomásszerzéstől számított három napon belül kell megszüntetni a munkaviszonyt. A rendkívüli felmondás indokát a munkáltatónak kell bizonyítania. A bizonyítás kérdése nagyon gyakran problematikus.

Amennyiben a második megoldást választja, akkor a munkáltató csak az üzemi megállapodásban (works regulation) előre meghatározott szankciók közül választhat. A bírói gyakorlat szerint a szankció alapjául szolgáló kötelezettségszegést nem kell kimerítően leírni az üzemi megállapodásban. Elegendő az általános meghatározás: pl. a munkavállaló megszegte a munkahelyi telekommunikációs szabályzatban írottakat, stb.

A gyakorlatban az egyik legnagyobb probléma az elkövető személyének a meghatározása. Az Internet lehetővé teszi, hogy a használója inkognitóban maradjon, sőt még azt is, hogy más nevében (más azonosítóját használva) lépjen be és tevékenykedjen a világhálón [pl. a munkatárs számítógépéről követ el Internet-rombolást vagy csalást (komputerkalózkodás)].

2.1. Felelősség a helytelen e-mail/Internet használatért

Kétfajta felelősség merülhet fel: a) az egyik a munkáltató és a munkavállaló között; a másik pedig b) a külső harmadik személlyel szemben fennálló felelősség.

A. A munkavállaló: A munkavállaló magánjogi felelősséggel tartozik mind a munkáltató, mind pedig külső harmadik személy felé az általa elkövetett csalásért (bedrog – dol), a súlyosan gondatlan magatartásáért (zware schuld – faute lourde) és az enyhe gondatlan magatartásáért (gewoonnlijke – lichte schuld – faute légere habituelle).[52]

Abban az esetben, ha a szerződés végrehajtása során a munkavállaló kimeríti valamely büntetőjogi tényállást, akkor büntetőjogilag is felelősségre vonható.

B. A munkáltató: A munkáltató a tevékenységével összefüggő minden kárért felelős, még akkor is, ha bizonyítja, hogy a kár bekövetkezését nem tudta megakadályozni.[53] A munkáltatót alapvetően objektív alapú felelősség terheli.

A 2000-ben módosított belga Büntető törvénykönyv négy új – az informatikával kapcsolatos – tényállást vezetett be: *a)* informatikai kijátszás, *b)* elektronikai csalás, *c)* az informatikai rendszerhez való engedély nélküli hozzáférés (Ezt mi leegyszerűsítve „internet-kalózkodásnak" nevezzük: beleértve a munkahelyen belüli kalózkodást is, ami akkor fordul elő, ha a munkavállalónak csak limitált hozzáférése van a rendszerhez és ezt növeli meg önhatalmúlag, illetve a külső kalózkodást is) és *d)* adat- és információszabotázs. Minden tényállás megállapításához szükséges a jogellenes szándék. Egyetlen kivétel ismert: a személyes adatokat tartalmazó adatbázis megrongálása (bestand – banque de données).

A felelősség előfordulásának eseteit – leegyszerűsítve – a következő táblázatban foglaltuk össze.

---

[52] Article 18 of the Statute on employment contracts.

[53] Article 1384, 3 Civil Code.)

1. sz. táblázat

	Munkáltató		*Munkavállaló*		*Külső harmadik személy*	
	Polgári	*Büntető*	*Polgári*	*Büntető*	*Polgári*	*Büntető*
Munkáltató	-	-	+	+	+	+
Munkavállaló	+	+	-	-	+	+
Külső harmadik személy	+	+	+	+	-	-

Forrás: Saját forrás

3. Az ellenőrzés technikai mikéntje

3.1. Felhatalmazás

Az e-mail/Internet használat engedélyezésének legjobb módszere, ha megalkotnak egy munkahelyi szabályzatot. Ebben alapvetően három kérdést kell érinteni: *a)* a felhasználó hozzáférése; *b)* a használat módja és *c)* a korlátozás/tiltás.

A szabályzatban meg kell határozni, hogy a munkavállalónak milyen információ és adat eléréséhez és felhasználásához van joga. Az e-mail/Internet használat célja a korrekt és felelősségteljes felhasználás elérése. Máig vitatott kérdés, hogy vajon magáncélra használható-e a munkahelyi elektronikus eszköz. Alapvetően négy lehetőség létezik: *a)* teljes tiltás; *b)* a használat csak sürgősségi (emergency) esetben, munkáltatói engedélyel; c) eseti használat engedélyezése, munkáltatói jóváhagyással; *d)* korlátozott felhasználás, amelynek a mértéke munkáltató szükségleteinek megfelelően alakul.

A tiltás tartalmi szempontból leginkább a következő kategóriákra vonatkozik: *a)* általános jellegű visszaélés (pl. játékra utaló vagy láncszerű levelek továbbítása stb.), *b)* tiltott témák (pornográfia, diszkriminatív jellegű oldalak látogatása stb.) és *c)* illegális használat (pl. Internet kalózkodás stb.).

3.2. A felelősség megállapításához szükséges, a felhasználás jellege szerinti különbségtétel

E-mail esetén a legegyszerűbb módszer, amikor a küldött levél végére odaírják, hogy melyik szervtől küldték, valamint azt, hogy ez egy üzleti levél, amelyet a küldő szerv ellenőrizhet.

Internet használat esetén könnyű különbséget tenni, ha a munkavállaló által felkeresett web oldal nyilvánvalóan nem kapcsolódik a munkáltató tevékenységi köréhez (pl. pornográf tartalmú honlap stb.). Sokkal bonyolultabb a megítélés, amikor az internetes

oldal általános jellegű információkat tartalmaz (pl. újságcikk, kormányzati oldal, hirdetések stb.).

3.3. Az ellenőrzés

Ha a munkáltató ellenőrizni kívánja a munkahelyi elektronikus kommunikáció forgalmát, akkor ezt a tényt, valamint az ellenőrzés módszerét, időpontját és a célját előre köteles közölni a munkavállalóval. Általánosan elfogadott felfogás, hogy a munkáltatónak nem szabad folyamatosan ellenőriznie a munkavállaló elektronikus kommunikációját, mert ezzel megszegi az arányosság elvét (proportionality) és túlterjeszkedik az eredeti célkitűzésen.

3.4. Az érdekképviseleti szervekkel történő konzultáció kérdése

Az 1983. december 13-án kelt 13. számú kollektív szerződés 2. cikkelyének 1. pontja kimondja, hogy „amennyiben a munkáltató elhatározta, hogy valamilyen új technológiát vezet be a munkahelyen – amely a munkavállalók többségének a munkavégzési körülményeit érinti –, akkor a bevezetés előtt köteles informálni a munkavállalói érdekképviseletet a bevezetendő új technológia főbb jellemzőiről, a bevezetés indokairól és az alkalmazás következményeiről."

Amennyiben a munkahelyen működik üzemi tanács, akkor a munkáltatónak értesíteni kell az üzemi tanácsot, az e-mail/Internet ellenőrzésre irányuló szándékáról. Az üzemi tanácsnak joga van véleményezni a tervet és tanácsot adhat a munkáltatónak. Abban az esetben, ha a bevezetendő új technológia a munkavállalók nagy számát érinti (legalább a munkavállalók 50 %-a vagy azonos szakmát űzők közül legalább 10 főt), akkor a munkáltatónak egy speciális eljárást kell követnie. Az eljárás lényege, hogy az új technológia bevezetése előtt legalább 3 hónappal kell értesíteni az üzemi tanácsot.

Amennyiben létezik szakszervezet az adott munkahelyen – függetlenül attól, hogy van-e üzemi tanács – a szakszervezetet is tájékoztatni kell a munkavállalók gazdasági és szociális érdekeit érintő technológiai változásokról.

A fentieken kívül a munkahelyi munkavédelmi bizottság/képviselő a munkáltató által bevezetendő elektronikus kontrollal kapcsolatban tanácsot adhat.

Németország

1. A munkáltató ellenőrzési joga

A munkáltató ellenőrzési joga alapvetően attól függ, hogy a munkavállaló az e-mail/internet használata a munkaköréhez tartozik-e vagy csak magáncélból használja azt. A munkahelyi e-mail/Internet ellenőrzés kérdésének Németországban még nincs kialakult bírói gyakorlata. Sok eseten analógiával a telefonhasználatra és a telefonbeszélgetések lehallgatására vonatkozó szabályokat tekintik kiindulási alapnak.

A szakértők között két dologban egyetértés mutatkozik: *a)* a munkáltatónak joga van a munkahelyi e-mail/Internet forgalmat ellenőrizni és *b)* ezt csak úgy teheti meg, hogy ezzel ne sértse meg a munkavállaló magánszféráját/személyiségi jogait.

Az üzleti e-mail-ek mindegyikét, teljes terjedelmében – a levél tartalmát és címzettjét egyaránt – ellenőrizheti a munkáltató. A munkavállaló tevékenységének az ellenőrzése a munkáltató munkajogból eredő jogosultsága. Az ellenőrzés alapvetően arra irányul, hogy a munkavállaló végrehajtotta-e a munkáltatói utasítást. A vizsgált esetben a munkavállaló az utasítás végrehajtását valamilyen elektronikus eszköz alkalmazásával végzi el. A munkáltató azt ellenőrzi, hogy a munkavállaló az elektronikus eszközök használata során a munkáltató által engedélyezett határon belül maradt-e. A jogi alaphelyzet nagyon hasonlít a hivatalos levél munkáltatói ellenőrzéséhez. Az alapvető különbség, hogy a munkavállaló oldaláról sokkal nagyobb a kísértés az elektronikus eszközök valamilyen illegális használatára, a munkáltató pedig jóval nehezebben tudja ellenőrizni a munkavállalót.

Általában a magáncélú e-mail-eket a munkáltató csak számolási céllal vagy a zavartalan működés ellenőrzése céljából ellenőrizheti. Alapesetben a levelezés tartalmába nem tekinthet bele.

1.1. Az ellenőrzés korlátjai

Az üzleti célú elektronikus média használatáról: *a)* alapvetően a személyiségi jogok védelméről rendelkező jogszabály (például Alaptörvény), míg speciális szabályként *b)* a Szövetségi Adatvédelmi Törvény rendelkezik.

A személyiségi jogok védelme a német Alaptörvény 1(1) és 1 (2) cikkelyeiben jelenik meg. A személyiségi jogok védelme egy független, szubjektív és individuális jog. Az Alkotmány ugyancsak védelemben részesíti a szabad cselekvéshez és a szabad döntéshozatalhoz való jogot. Szintén előírja még a beszédben elhangzottak bizalmas kezeléséhez való jogot és az információkkal való önrendelkezés jogát. Összefoglalva az összes személyes adat védelméhez való jogot.

Ezen kívül, a német Alaptörvény 10. cikkelye garantálja a levelezés és a telekommunikáció védelmét. Ezen kívül a Telekommunikációs törvény 85. Szakasza minden olyan személyt vagy szervet, aki elektronikus kommunikációs szolgáltatásokkal foglalkozik kötelezi, hogy a személyiségi és a magánszféra védelméhez való jogokat részesítse védelemben és a telekommunikációs és levéltitkot tartsa tiszteletben.[54]

A Német Szövetségi Alkotmánybíróság és a Szövetségi Munkaügyi Bíróság kimondta, hogy a munkavállalók saját maguk határozhatják meg, hogy kinek biztosítanak jogot ahhoz, hogy a kommunikációjukat – beleértve a verbális és az elektronikus kommunikációt is – ellenőrizhessék. A munkáltató által végzett mindennemű titkos megfigyelés a munkavállalók személyiségi jogát sérti, kivéve, ha az ellenőrzésre a munkáltatónak alapos indoka – pl. bűncselekmény elkövetésének alapos gyanúja, a munkáltató jó hírének csorbítása, üzleti titok megsértése stb. – volt. A fent ismertetett bírói jog munkavállaló-barát értelmezése – amely álláspontot végül nem fogadták el a gyakorlatban – szerint, az üzleti tartalmú e-mail közelebb áll a telefonhíváshoz, mint a postai úton küldött üzleti levélhez. A bírói esetjog szerint az üzleti telefonhívások titkos lehallgatása nem engedélyezett. Ennek az okát abban jelölik meg, hogy a telefonos beszélgetés az egy verbális párbeszéd, amelyet a felek nem képesek utólag rekonstruálni és ellenőrizni, mint egy írott levelet, ugyanakkor bármikor megvan a lehetőségük arra, hogy a mondot-

[54] Working document on the surveillance of elctronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 28.

takat megváltoztassák. Ezzel szemben az e-mail maradandó, hiszen először meg kell írni és csak utána továbbítható. Az elküldést követően is megmarad. A levél tartalmát a küldő és a címzett egyaránt megismerheti és ha elmenti, akkor később bármikor rekonstruálhatja. Ezért az e-mail-t az írott dokumentummal – hagyományos levél – azonos módon lehet kezelni.

A Szövetségi Adatvédelmi törvény nem tartalmaz a fent vázolt általános személyiségi jogi védelmen kívüli speciális és szélesebb körű védelmet a munkavállalók számára. A törvény felfogásában az e-mail személyes adatokat tartalmaz, mivel az e-mail lehetővé teszi az e-mail írójának és fogadójának az azonosítását.[55] A törvény két esetben engedélyezi az adatok gyűjtését, feldolgozását és felhasználását: *a)* ha jogszabály írja elő vagy *b)* az érintett személy beleegyezésével történik.[56]

Az elektronikus médiák privát célú használatának ellenőrzése még szigorúbban korlátozott a munkáltató számára, mint az üzleti célú felhasználás ellenőrzése. Ilyen esetben a telekommunikáció titkosságára is figyelemmel kell lenni. Erről a Telekommunikációs törvény (TKG) és a Teleservices Data Protection törvény (TDDSG) rendelkezik.

A Telekommunikációs törvény (TKG) csak abban az esetben védi a telekommunikáció titkosságát, ha a szolgáltatást valamely külső szolgáltató, üzleti alapon biztosítja. Ebben az esetben nem lehet csak üzleti célú használatot engedélyezni és minden magán célú felhasználást megtiltani. A TKG hatálya alá tartozó esetekben számlálás, javítás és a szolgáltatás zavarmentességének vizsgálata céljából, az adatgyűjtés és adatfeldolgozás engedélyezett. Ilyen esetekben sem engedélyezett a küldött kommunikációs anyag tartalmának az ellenőrzése, kivéve ha arra valamilyen alapos ok (pl. bűncselekmény elkövetésének a gyanúja stb.) szolgál.[57]

A titkosság elve védi a telekommunikációban résztvevő felek helyzetét (pl. ki beszélt kivel, mikor stb.). A titkosság biztosítása érdekében magáncélú telekommunikáció ellenőrzését a minimálisra kell szorítani. Abban az esetben, ha a munkáltató ellenszolgáltatás nélkül engedélyezi valamennyi telekommunikációs eszköz és időkorlát nélküli használatát – ez a leginkább elterjedt gyakorlat –, ilyenkor a továbbított adat nem ellenőrizhető. Ez alól kivételt csak a telekommunikációs rendszer működésének az ellenőrzése jelenti, de ilyenkor sem az adatokat elemezni, csak a továbbításra szolgáló hardware és software ellenőrzése végezhető el.

A másik eset, amikor a munkáltató magáncélú Internet használatot engedélyezett és a telekommunikációs rendszert a munkáltató – és nem külső szolgáltató – biztosítja. Ez a kapcsolat a TDDSG törvény hatálya alá tartozik. A törvény 6. § (1) értelmében csak olyan mértékben lehet adatokat gyűjteni és feldolgozni, amely lehetővé teszi a felhasználó számára a kommunikációs rendszer zavartalan használatát, illetve a munkáltató számára, hogy ez alapján kiszámíthassa a munkavállalót terhelő e-mail/Internet használat díját. Ha a munkavállaló privát célra is ingyenesen használhatja a rendszert, akkor a munkáltatónak nincs semminemű jogalapja az ellenőrzésre, kivéve, ha a munkavállaló ebbe beleegyezett.

[55] Federal Data Protection Act (BDSG) 3. § (1).
[56] Federal Data Protection Act (BDSG) 4. § (1).
[57] TKG 85. § (3) 4. mondat.

2. Szankciók

Ha a magáncélú felhasználás tiltott és a munkavállaló megszegi ezt a tilalmat, akkor figyelmeztetésben részesíthető. Ha ezt követően sem tartja be az előírást, akkor a munkaviszony – a munkavállalónak felróható okból – megszüntethető. Ugyanez a szankció alkalmazható akkor is, ha a munkavállaló munkaközi szünet alatt e-mailezik vagy szörfözik az interneten. Az alapul szolgáló jogi helyzet leginkább a munkahelyi magáncélú telefonhívások megítéléséhez hasonlít.

Abban az esetben, ha a magáncélú használat – valamely belső szabályzat vagy a vállalati szokás alapján – engedélyezett, akkor e-mail/Internet használat miatt a munkaviszonyt csak kivételes esetekben lehet megszüntetni. Pl. a munkavállaló e-mail/Internet használata messze meghaladja az általában elvárható normális mértéket, amelyet a munkáltató már nem kíván finanszírozni. Ugyanakkor, ha a munkáltató mégis engedélyezi vagy jóváhagyja a túlzottnak tűnő használatot, akkor erre hivatkozással a munkaviszonyt nem lehet megszüntetni. Az ilyen jóváhagyó beleegyezést nem lehet vélelmezni akkor, ha a munkavállaló a számára előírt határidőt az intenzív magáncélú e-mail/Internet használat miatt nem tudta betartani, vagy a használat már nagyon magas költséget okoz a munkáltatónak vagy fizikailag túlterheli a rendszert. Még ilyen ügyben nem született ítélet a német Legfelsőbb Bíróságon. Ugyanakkor, alacsonyabb szintű bíróság kimondta, hogy amennyiben a munkáltató kifejezetten nem tiltotta a magáncélú Internet használatot, akkor az évi 100 óra magáncélú szörfözés még nem alapozza meg a munkaviszony azonnali hatályú felmondását. Azonnali hatályú megszüntetés alapja lehet azonban, ha az e-mail/Internet segítségével bűncselekményt követnek el vagy szexuálisan zaklatják a munkatársaikat.

2.1. A jogellenes használat jogkövetkezményei

Az írásos figyelmeztetés vagy elbocsátás mellett a munkáltató vagyoni kártérítési igénnyel fordulhat a munkavállalóval szemben. Ez olyan esetben fordulhat elő, amikor a nem engedélyezett e-mail/Internet használat eredményeként a munkáltatónál tényleges kár – pl. vírusfertőzés miatt fontos üzleti információkat veszít el, vagy ennek következtében kára származik; az elpusztult számítógép kijavítása eltart egy ideig és ezen időtartamra elesik a bevételtől stb. – következik be. Ilyenkor a kereset jogalapja nem kizárólag csak a munkaszerződés megszegéséből származhat, hanem a BGB 823. §-ából, amely a jogellenes magatartás tanúsításáról rendelkezik. Abban az esetben, ha a munkáltató figyelmezette a munkavállalót az esetleges vírusveszélyre és annak a lehetséges következményeire – pl. az „X" elnevezéssel beérkező levelet ne nyissa meg, mert veszélyes lehet – és a munkavállaló ennek ellenére folytatta a tevékenységét, akkor a munkavállaló súlyos gondatlanságát lehet állapítani.

További probléma, hogy ilyen esetben nagyon nehéz pontosan megállapítani a kár mértékét. Ennek az elkerülését szolgálja az a megoldás, hogy ilyenkor a munkáltató igyekszik szerződéses felelősségi (kontraktuális felelősség) alapra helyezni az ügyet. Ilyenkor a munkavállaló a munkaszerződésében meghatározott személyi alapbéréig vagy a minimálbérig felel.

Abban az esetben, ha a munkáltató szegi meg a kötelezettségét és jogellenesen gyűjt adatokat vagy ellenőrzi a kommunikációt, akkor az így szerzett információkat nem lehet bizonyítékként felhasználni a bíróság előtt. Ezen túlmenően, a munkavállaló keresettel

fordulhat a bírósághoz, amelyben azt kéri, hogy a munkáltató szüntesse be a jogellenes magatartását és az illegális megfigyeléssel szerzett adatokat semmisítse meg, továbbá kártérítést is követelhet.

3. Az ellenőrzés technikai mikéntje

3.1. A magáncélú és a hivatalos célú levelezés engedélyezése, elhatárolása és ellenőrzése

Annak az engedélyezése, hogy a munkahelyi elektronikai eszközöket, valamint az e-mail/Internet elérhetőséget a munkavállaló csak üzleti és vagy magáncélra is alkalmazhatja a munkáltató hatásköre. A munkaszerződés rendszerint nem tartalmaz magáncélú használatra szóló felhatalmazást a munkavállaló javára. Amennyiben a munkáltató mégis engedélyez ilyen használatot, akkor annak a tényét és a feltételeit vagy a munkaszerződésben vagy az üzemi tanáccsal kötött üzemi megállapodásban rögzítik.

Ugyanakkor, vészhelyzet esetén a munkavállaló külön engedély nélkül is használhatja a munkáltató telefonját vagy más elektronikai eszközeit.

Különbséget nemcsak a magáncélú és az üzleti használat között kell tenni, hanem ezen belül a magáncélú felhasználás – érzékeny kritériumok alapján – további szegmensekre bontható. A magáncélú használat engedélyezése a munkáltató diszkrecionális döntése. Ezért a megadott engedély bármikor visszavonható. A visszavonásnál mindig figyelemmel kell lenni a diszkrimináció tilalmát kimondó jogszabályokra. Gyakorlati tapasztalatok alapján a következő feltételeket célszerű rögzíteni: *a)* az e-mail/inteernet használat maximumát (pl. napi 15 perc.); *b)* a használat időpontjá(i)t (pl. munkaközi szünetben és nem a tényleges munkavégzés ideje alatt.); *c)* a költségek viselését; *d)* a tartalmat (pl. nem lehet pornográf, emberiség ellenes stb.) és *e)* a forgalmazott adatok vagy dokumentumok maximális nagyságát.

Az illegális internethasználat elkerülése végett a munkáltatónak célszerű olyan filter programokat (software) vásárolni, amelyek a nemkívánatos – munkavégzéshez nem kapcsolódó – honlapok használatát megakadályozzák. Ennek a módszernek az alkalmazásakor a munkavállaló személyiségi jogai sem sérülnek.

Annak érdekében, hogy a munkáltató minél hatékonyabban ellenőrizhesse az üzleti leveleit, célszerű az üzleti és a magánjellegű levelezést teljesen szétválasztani. Ez különböző módszerek segítségével történhet, például a munkavállaló két titkos kóddal rendelkezik. Az egyik a munkaköréhez tartozó üzleti jellegű tevékenységek folytatásához, míg a másik a magáncélú használat idejére szolgál. Másik megoldás, hogy a munkavállalónak szerződéses kötelességévé kell tenni, hogy ráírja a magáncélú leveleire, hogy privát vagy magánjellegű stb. és a lehető legrövidebb időn belül törölje azokat a munkahelyi számítógépének a memóriájából. Amennyiben a munkavállaló ezen megállapodás ellenére nem jelzi a levélen annak a rendeltetését, akkor a munkáltató – mivel nincs róla tudomása – jogszerűen ellenőrizheti a magáncélú leveleit is. A munkavállaló titkosíthatja a magáncélú leveleit. Ilyen esetben a munkáltató csak különösen indokolt esetben – pl. bűncselekmény elkövetésének alapos gyanúja – dekódolhatja a munkavállaló privát e-mail-jét.

3.2. A munkavállalói érdekképviseletekkel történő konzultáció

A német Üzemi Alkotmányról rendelkező törvény (Works Constitution Act – BetrVG) 87. § (1) bekezdése értelmében az üzemi tanácsnak minden olyan esetben joga van az együttdöntésre, amikor a munkáltatói döntés az üzleti tevékenységgel vagy a munkavállalók vezetésével összefüggésbe hozható. Ugyanakkor az olyan döntésekbe, amelyek konkrétan a munkavállaló tevékenységét határozzák meg az üzemi tanácsnak nincs beleszólása (együttdöntési joga). Ha egy munkáltató engedélyezi a munkahelyi e-mail/Internet rendszerek magáncélú felhasználását, akkor ezt a döntést meg kell vitatni az üzemi tanáccsal és az üzemi megállapodásban kell rögzíteni.

A BetrVG törvény 87. § (1) 6. pontja értelmében, a munkavállaló elektronikus kommunikációjának az ellenőrzését végző berendezés beszerzés olyan döntés, amely az üzemi tanács hatáskörébe tartozik. Az üzemi tanács együttdöntési jogosultsága – ebben a vonatkozásban – a munkavállalók személyiségi jogainak a megőrzését és védelmét szolgáló garanciaként szolgál. A munkavállalóknak ezt a jogát elsősorban a munkáltató egyoldalú döntéseivel szemben kell védeni.

Ugyanakkor az üzemi tanácsnak nincs semmilyen jogosultsága arra, hogy meghatározza azt, hogy a munkáltató milyen telekommunikációs eszközt használhat vagy vásárolhat. Ennek az eldöntése teljesen a munkáltató hatáskörébe tartozik.

Az üzemi megállapodás rögzíti ugyan az e-mail/Internet használat feltételeit, de nem ad korlátlan manőverezési lehetőséget a felek számára. A megállapodásban szereplő megengedett ellenőrzés – üzleti célú kommunikáció és használat esetén – nem érintheti hátrányos módon a munkavállalót megillető személyiségi jogokat. A magáncélú levelezés esetén a telekommunikációs törvény határozza meg a jogszerű ellenőrzés kereteit, de ez sem sértheti az alapvető emberi jogokat.

Még egyszer kihangsúlyozzuk, hogy a magáncélú e-mail/Internet használat engedélyezéséhez és az engedély terjedelmének a meghatározásához nem kell az üzemi tanács beleegyezése (co-determination). Ez a munkáltató hatáskörébe tartozik. Ugyanakkor, ha a munkáltató engedélyezte a privát használatot, akkor az üzemi tanácsnak már együttdöntési joga van az alkalmazható ellenőrzési eszköz megválasztásában, az ellenőrzés végrehajtásában és azért is felelősséggel tartozik, hogy az ellenőrzés mindenkor megfeleljen a hatályos jogszabályoknak.

Összefoglalva: Németországban a magáncélú és a hivatali telekommunikáció jogi védelmében eltérés található. A hivatali elektronikus levelezés ellenőrzése megengedett. Ugyanakkor, a munkavállaló kifejezett beleegyezése nélkül nem lehet a munkahelyi hivatalos levelezést megfigyelni és ellenőrizni, majd az így kapott adatokat a munkavállaló munkateljesítményének az értékelésére felhasználni. A jogszerű megfigyeléshez szükséges az üzemi tanács beleegyezése. Ugyanakkor a magánjellegű elektronikus levelezés megfigyelése és különösen a küldött vagy fogadott levelek elolvasása szigorúan tilos. Az ellenőrzés és megfigyelés jogszerűségének betartása érdekében praktikusan úgy lehet a problémát kiküszöbölni, ha teljesen elkülönítik a munkahelyen folytatott hivatalos és magánlevelezést.

Előzetes értesítés nélkül engedélyezett az elektronikus kommunikáció megfigyelése és ellenőrzése, amely a rendszer működésének garantálása miatt szükséges (pl. rendszeres ellenőrzés a vírusfertőzés kiküszöbölésére stb.).[58]

Hollandia

1. A munkáltató ellenőrzési joga

a) A holland alkotmány 10. cikkelye kimondja, hogy mindenkinek joga van ahhoz, hogy a magánszféráját tiszteletben tartsák.[59]

b) A Polgári törvénykönyv. A holland polgári törvénykönyv 660. cikkelye alapján a munkáltató – a gazdasági érdekeinek előmozdítása, a minél fegyelmezettebb és hatékonyabb munkavégzés elérése érdekében – utasíthatja a munkavállaló(ka)t. Az utasítási jog magában foglalja az elvárható és követendő munkahelyi magatartás munkáltató általi meghatározásának a jogát. A munkaviszonyban rendszerint jelenlévő alá-fölérendeltségi viszony miatt a munkavállalónak a munkáltatói utasításokat végre kell hajtani.

A Polgári törvénykönyv 611. cikkelye foglalkozik a munkáltató és a munkavállaló között fennálló jogviszony tartalmának elvi kérdéseivel. Az alkotmányban foglalt garanciális szabály alapján a Ptk. 611. cikkely tartalmába beleértik a munkáltató azon kötelezettségét, hogy köteles tiszteletben tartani a munkavállaló személyiségi jogait és a magánszféráját.

A munkahelyi e-mail/Internet használat vonatkozásában – beleértve a használat szükséges korlátozását is – a munkáltatónak joga van belső szabályzat kiadására.

c) Munka törvénykönyve (Arbeidsomstandighedenwet). További releváns szabályozást tartalmaz a holland Munka törvénykönyve. A holland Mt. 3 cikkelye kimondja, hogy a munkáltató olyan optimális munkafeltételeket köteles biztosítani és a munkát oly módon köteles megszervezni, hogy ezzel a munkavállalók egészsége és biztonsága nem kerülhet veszélybe. A munkáltató kötelessége, hogy a munkavégzéssel összefüggő veszélyeket, kockázatokat – preventív eszközök alkalmazásával – a lehető legnagyobb mértékben csökkentse. A munkáltató ezen általános kötelezettsége az Mt. több, a munkavégzés feltételeit szabályozó, konkrét cikkelyében konkretizálódik.

d) A munkafeltételekről rendelkező törvény (Working Conditions Act) 5.1–5.3 cikkelyei kimondják, hogy a munkavállalót értesíteni kell a munkavállalói megfigyelésről vagy ellenőrzésről. A munkavállalón kívül a szakszervezetet vagy az üzeni tanácsot is értesíteni kell. Ezeknek a szervezeteknek meghatározott esetben egyetértési joguk van. Ezen kívül az Üzemi Tanácsról rendelkező törvény (Working Council Act) külön is kiemeli, hogy a munkavállaló megfigyeléséről az üzemi tanácsot informálni kell és ilyen esetekben az üzemi tanácsnak egyetértési joga van.[60]

e) A személyes adatok védelméről rendelkező törvény (Wet Bescherming Persoonsgegevens WBP). Ez az ötödik olyan jogforrás, amely a munkavállalók elektronikus kommunikációjának a megfigyeléséről rendelkezik. Az adatvédelmi törvény 8. cikkelye kimondja, hogy csak olyan esetben végezhető ellenőrzés, ha ahhoz a megfigye-

[58] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 28–29.

[59] I. m. p. 32.

[60] I. m. p. 32.

lést végző szervnek (jelen esetben munkáltatónak) vagy külső harmadik személynek valós érdeke fűződik. Ugyanakkor ezen ellenőrzési tevékenység során a munkavállaló alapvető jogai – beleértve az alapvető emberi jogai, valamint a magánszféra védelméhez való jogot – nem sérülnek. A törvény meghatározza az adatgyűjtéssel, feldolgozással és felhasználással megbízott személy kötelezettségeit. A munkaviszony esetén ez a személy a munkáltató lesz. Ő felel az adatgyűjtés, feldolgozás és felhasználás jogszerűségéért. A munkáltatónak van tehát joga arra, hogy a munkavállalói e-mail/Internet forgalmazást ellenőrizze. Egyre gyakrabban felmerül az a kérdés, hogy vajon a munkáltatónak van-e joga személyes jellegű információk, adatok gyűjtésére, amelyet később a munkavégzés során a munkavállalóval szemben felhasználhat.

1.1. Az ellenőrzés korlátjai

A vázolt dilemma előrevetít egy olyan láthatatlan (képzeletbeli) demarkációs vonalat, amelyet a munkáltatónak nem szabad átlépnie. Ezen a képzeletbeli vonalon túl nem gyűjthető a munkavállalóra vonatkozó személyes adat. Ebből az is következik, hogy a munkáltatónak nem lesz felhatalmazása arra, hogy a munkahelyen folyó e-mail/Internet forgalmazást teljes körűen és következetesen ellenőrizhesse. A munkáltatónak meg kell jelölnie azokat a célokat, amelyeket az ellenőrzés során el kíván érni, valamint meg kell jelölnie, hogy milyen természetű adatokat kíván összegyűjteni.

A munkahelyi e-mail/Internet forgalmazás során el kell határolni a küldött e-mail funkcióját és célját. Egyszerűbben fogalmazva azt kell eldönteni, hogy a konkrét ellenőrzés esetén kizárólag üzleti levélről van szó, vagy abban – teljesen vagy részben – megjelennek magánjellegű elemek is. Ezt minden esetben a munkáltató dönti el. Ő határozza meg, hogy a munkavállaló csak üzleti célra használhatja a munkáltató eszközeit, vagy a munkáltató által engedélyezett keretek között a magáncélú felhasználás is engedélyezett.

Amennyiben a munkáltató bizonyos mértékű magáncélú felhasználást is engedélyezett, akkor a munkáltatónak célszerű egy belső telekommunikációs szabályzatot megalkotni. A szabályzat megalkotását követően a munkáltató jogszerűen végezhet a munkavállaló e-mail/Internet használatára vonatkozó ellenőrzést. Az ellenőrzés során azt vizsgálják, hogy vajon a munkavállalók betartották-e a belső szabályzatban meghatározott szabályokat. Az ilyen ellenőrzés alapvetően jogszerű lesz a munkáltató részéről.

Az ellenőrzés mindig jogszerű, ha a munkáltató olyan információk birtokába jut, amely alapján joggal és alaposan feltételezhető, hogy a munkavállalók pornográf vagy rasszista tartalmú levelet küldenek, illetve honlapot látogatnak. Az ellenőrzést mind időben, mind pedig tartalmában korlátozni kell.

Ezen korlátozás következményeként a munkáltatónak ún. „jó munkáltatóként" kell viselkednie és úgy kell eljárnia, ahogy az a jó munkáltatótól általában elvárható.[61] A jó munkáltatótól általában elvárható magatartás azt jelenti, hogy munkáltató ok nélkül nem zaklatja, ellenőrzi a munkavállalóit, vagyis nem sérti meg a magánszférához való jogukat és az alapvető személyes szabadságjogaikat. Az e-mail/Internet ellenőrzés mértéke csak korlátozott és arányosított (proportional) lehet. (Csak a jogszerűen indokolható mértékig (justifiable need) terjed ki.)

[61] BW. 7:611. cikkely.

Alapvető szabályként érvényesül, hogy a munkáltatónak először minden egyéb információ szerzési forrást ki kell merítenie és csak a legvégső esetben alkalmazhat elektronikus megfigyelést. Amennyiben más, kevésbé érzékeny eszközzel is elérető a kitűzött cél, akkor a munkáltatónak először azokat kell kimerítenie és csak végső megoldás lehet a megfigyelés.

2. Szankciók

A jogszabályok, illetve a vállalati belső szabály(ok) megsértése különböző súlyú szankcióval jár. Az egyszerű figyelmeztetéstől kezdve az azonnali hatályú jogviszony megszüntetésig.

Természetesen mind a vállalati elektronikus kommunikációra vonatkozó szabályzatot, mind pedig a kiszabható szankciókat a helyben szokásos módon és minél szélesebb körben meg kell ismertetni a munkavállalókkal. Ez a kötelezettség a munkáltatót terheli. A szabályzatnak és a végrehajtására vonatkozó eljárási rendnek jól kidolgozottnak kell lennie, amelyet a munkáltatónak is minden esetben korrektül és következetesen be kell tartania. Az ilyen munkáltatói magatartás az egyik fontos záloga annak, hogy a munkavállalók is komolyan vegyék az abban írottakat és kövessék azokat. A következetlen munkáltatói magatartás elbizonytalanítja a munkavállalókat és erősen az önkéntes normakövetés ellen hat.

Ha a munkáltató a jogszabályok vagy a munkahelyi szabályzat előírásait megszegve gyűjt adatot vagy végez megfigyelést, az így szerzett információkat a bírósági eljárásban nem használhatja fel. Másképpen fogalmazva, a bíróság a jogellenesen gyűjtött adatokat nem fogadja el a bizonyítási eljárásban. A visszautasítás indoka az lesz, hogy a munkáltató megszegte a normát és nem jóhiszeműen jár el.

A másik jogorvoslati lehetőség, hogy a bíróság felszólítja a munkáltatót, hogy a jövőben tartózkodjon az ilyen jogellenes magatartástól. Ha mégsem tenné, akkor büntetés kiszabására kerül sor.

3. Az ellenőrzés technikai miként je

A fentiekből is világosan következik, hogy a munkáltatónak meg kell alkotni a munkavállalók e-mail/Internet használatára vonatkozó szabályzatát. A szabályzat tiszta és kiszámítható helyzetet teremt mind a munkavállalók, mind pedig a munkáltató magatartására nézve. Pontosan meghatározza a felek jogait és kötelezettségeit. Az esetjogból kiderül, hogy a bíróságok eljárásuk során alkalmazzák a szabályzatot, különösen az abban rögzített szankciórendszert.

A bírósági gyakorlatból arra is lehet következtetni, hogy nagyon bizonytalanná válik a felmerülő konfliktusok megítélése, ha a munkahelyen nem alkottak ilyen szabályzatot. Szabályzat hiányában mind a munkavállaló, mind a munkáltató, de még a bíróság is bizonytalan talajon mozog.

A munkahelyen alkotott szabályzatot be kell mutatni a holland Személyiségi Jog Védelmét Ellátó Testülethez (College Bescherming Persoonsgegevens). A testület megvizsgálja, hogy a szabályzatban foglaltak megfelelnek-e a Holland Személyiségi Jog Védelméről rendelkező törvény (Netherlands Privacy Act – WBP) előírásainak. Magától értetődik, hogy nagyobb a kikényszeríthetősége az olyan szabályzatnak, amely maradéktalanul megfelel a törvény előírásainak.

A holland Személyiségi Jog Védelmét Ellátó Testület (Adatvédelmi Hatóság) 1999. es határozatában kifejtette, hogy a munkavállaló folyamatos megfigyelése alapvetően tilos. Ha a megfigyelésnek valamilyen speciális vagy nyomós oka van, akkor más lesz a magatartás megítélése. Ezt a határozatot kell követni akkor is, ha a munkáltatói kommunikációs szabályzata tisztán kimondja, hogy a munkavállaló nem várhatja el, hogy a személyiségi jogait és a magánszféráját a munkahelyen belül védelemben részesítsék.[62]

Az üzemi tanácsnak (Ondernemingsraad) egyetértési joga van[63] a szabályzat elfogadása, módosítása és megszüntetése vonatkozásában. Ez annyit jelent, hogy a munkáltatónál minden olyan szabályzat, amely kapcsolódik a munkavállalókra vonatkozó személyes adatgyűjtéshez, adatfeldolgozásához vagy adatvédelemhez csak az üzemi tanács egyetértésével fogadható el. Ez a jogosítvány minden olyan munkahelyi elektronikus megfigyelési/kontroll rendszerhez kapcsolódik, amely segítségével megfigyelést, ellenőrzést, jelenlétet és a munkavállalói viselkedést lehet ellenőrizni.

Záró felvetésként megemlítünk egy új jelenséget. A Harlem-i Regionális Bíróság 2000. június 16.-án kelt ítéletében utalt a „munkahelyek privatizációjára", vagyis arra a jelenségre, hogy napjainkban egyre inkább kezd elmosódni a határ a munkahelyi szféra és a magánszféra között. A bíróság álláspontja szerint ebben az új kontextusban a munkavégzés során felmerülő magánjellegű kommunikációt engedélyezni kell.[64]

Egyesült Királyság

1. A munkáltató ellenőrzési joga

Nagy Britanniában a munkáltató csak korlátozott mértékben ellenőrizheti a munkavállaló munkahelyi e-mail/Internet használatát. A munkajogi szakértők azt javasolják a munkáltatóknak, hogy foglalják szerződésbe vagy alkossanak belső szabályzatot az e-mail/Internet használatról, ugyanakkor minden munkáltatónak tisztában kell lennie azzal a ténnyel, hogy a már meglévő vonatkozó jogszabályok számtalan tiltást és korlátozást tartalmaznak. A következőkben ennek a jogi szabályozásnak a főbb vonalait tekintjük át.

1.1. A nyomozásról rendelkező törvény (Investigation Powers Act, 2000)

A törvény alapelvi érvénnyel kimondja, hogy a kommunikáció lehallgatása alapvetően tilos. A törvényt a munkaviszonyra is alkalmazni kell. A törvény a következő kivételes esetekben engedi a munkáltatónak, hogy megfigyelje a munkavállalói e-mail/Internet kommunikációját:

a) mindkét fél (küldő és fogadó fél) beleegyezik a munkáltatói megfigyelésbe,
b) a lehallgatás a telekommunikációra vonatkozó jogszabályok (2000) – Lawful Business Practice; Interception of Communications – értelmében megengedett.

[62] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 32.
[63] Art. 27 WOR – Netherlands Works Council Act.
[64] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 32.

A jogszerű üzleti magatartásról rendelkező törvény (Lawful Business Practice Regulations, 2000) kivételesen lehetővé teszi – amennyiben specifikus és legitim célok indokolják – a munkavállaló munkahelyi elektronikus kommunikációjának az engedély nélküli lehallgatását. Amennyiben a lehallgatás mégsem esne a megengedett keretek közé, akkor a munkáltató magatartása jogellenes lesz. A jogsértő magatartás mind büntetőjogi, mind polgári jogi felelősséget von maga után.

A Lawful Business Practice Act 4. szakasz 2. bekezdése értelmében a munkáltató a következő esetekben végezheti legálisan a munkavállalók elektronikus úton történő kommunikációjának a megfigyelését:

- megfigyelési és adatrögzítési célból,
- bizonyítékgyűjtési célból,
- a felállított munkahelyi standardok, eljárási szabályok betartásának a figyelemmel kísérése,
- nemzetbiztonsági érdekből,
- bűncselekmény megelőzése vagy felderítése érdekében,
- a telekommunikációs eszközök, illetve rendszerek engedély nélküli használatának a felderítésére,
- a munkahelyi biztonság és a hatékonyság növelése érdekében,
- olyan célú megfigyelés, amelynek az a célja, hogy a munkáltató eldönthesse, hogy az adott információ, illetve adat üzleti vagy privát jellegű,
- az anonim telefonos segélyvonalak kommunikációjának a megfigyelése.

A kivételek köre meglehetősen széles. Ugyanakkor fő szabályként azt írja elő a törvény, hogy a megfigyelés akkor lesz igazán jogszerű, ha a munkáltató – a körülmények összességének figyelembe vételével – minden tőle elvárható erőfeszítést megtesz annak érdekében, hogy a potenciális telekommunikációs eszköz, illetve rendszer használókat értesítse a megfigyelés tényéről (3.2. szakasz).

1.2. Az adatvédelmi törvény (Data Protection Act, 1998)

Az Adatvédelmi törvény az élő személyre vonatkozó információk gyűjtésére, feldolgozására, tárolásra és kiadására vonatkozó eljárási szabályokat tartalmazza. A törvény hatálya kiterjed a személyes adatok védelmére, amelyek nagy valószínűséggel minden munkaviszonyban – a munkára jelentkezéstől a munkaviszony megszüntetéséig, sőt még tovább is – megtalálhatók. Az adatvédelmi (jelenleg informatikai) biztos által 2000 októberben kiadott Eljárási Kódex tervezetben (Code of Practice) számos az e-mail/Internet használatra vonatkozó rendelkezés található. A Kódex releváns szabályait a következőkben foglaljuk össze:

1.2.1. A megfigyelés általános standardjai

Ezek a standardok mindennemű munkáltatói megfigyelésre vonatkoznak.

- A munkáltatónak olyan speciális üzleti célokkal (érdekekkel) kell rendelkeznie, amely a megfigyelést indokolja.
- A munkáltatónak – a megfigyelés megkezdése előtt – minden esetben mérlegelnie kell, hogy a megfigyelés hogyan hat a munkavállalók magánszférájára, önbecsü-

lésére, autonómiájára és más jogaira. Az arányosság elve, vagyis a munkáltató nem alkalmazhat olyan módszert, amelynél a munkavállalókra gyakorolt negatív hatás meghaladja a megfigyeléssel elérni kívánt munkáltatói célkitűzést.

- Az arányosság elvének betartása és annak mérlegelése során a munkáltatónak célszerű konzultálnia az illetékes szakszervezettel vagy más munkavállalói érdekképviseleti szervvel.
- A munkáltatónak jegyzőkönyvben vagy egyéb maradandó módon rögzítenie kell az elérni kívánt üzleti célt, illetve és a munkavállalókra vonatkozó hatástanulmány eredményét.
- Amennyiben más módszer alkalmazásával megközelítőleg ugyanolyan eredmény érhető el, de kisebb lesz a munkavállalókat érintő negatív hatás, akkor a másik – kevésbé hátrányos – módszert kell alkalmazni.
- A szükségesség és a proporcionalitás elvét a monitoros megfigyelésekre is alkalmazni kell. Jogszerűtlen lesz a munkáltató magatartása abban az esetben, ha a megfigyelés célja csak bizonyos munkavállaló(k)ra irányul, de a munkáltató mégis folyamatosan az egész munkavállalói kört megfigyelés alatt tartja.
- A minden munkavállalót korrekt módon informálni kell arról, hogy a munkahelyen mikor, mire vonatkozóan történik adatgyűjtés vagy megfigyelés. Ettől a tájékoztatási kötelezettségétől a munkáltató csak kivételes esetben térhet el.
- Tilos a megfigyelés eredményét más – az eredeti céltól eltérő, amelyről a munkavállalókat nem informálták – célra felhasználni. Kivéve, ha a munkáltató nem utasíthatja vissza az adatszolgáltatást, pl. bűncselekmény elkövetése vagy tömeges rendbontásban való részvétel stb.

A munkáltatónak mindig tisztában kell lennie azzal, hogy a megfigyelés, feldolgozás stb. során – elsősorban technikai, de elképzelhető emberi mulasztás miatt is – a megszerzett adatok helytelenül (jogellenesen) kerülnek felhasználásra. Abban az esetben, ha ez a hiba ismert a munkáltató előtt és ez a munkavállalóra nézve hátrányos következményekkel járhat, akkor a munkáltatónak haladéktalanul informálnia kell erről a munkavállalót és mindent meg kell tenni annak érdekében, hogy a hibát helyrehozzák.

1.2.2. Rejtett megfigyelés

A Kódex kihangsúlyozza, hogy a titkos megfigyelés kérdése azért nagyon nehéz, mert éppen jellegéből következően az érintett munkavállalók rendszerint nem is tudnak róla. Ugyanakkor a Kódex arról is rendelkezik, hogy a teljesítmény titkos megfigyelése nagyon nehezen minősíthető jogszerűnek. A titkos megfigyelést csak nagyon szűk körben lehet legálisnak tekinteni. Ilyen lehet például, amikor ezzel bűncselekmény elkövetését előzik meg stb.

1.2.3. A Kódex e-mail megfigyelésre vonatkozó szabályai

a) Az elektronikus levelek tartalmát alapvetően nem tekintheti meg a munkáltató. Kivéve, ha nyilvánvaló, hogy a rögzített és később kinyomtatott e-mail nem elegendő, és a munkáltatónak az aktuális e-mail forgalmazás azonnali megfigyelésére jól megfontolt üzleti érdeke szolgál.

b) Megfigyelés esetén is csak az üzleti tartalmú információkra szabad koncentrálni. Annak az eldöntésénél, hogy megtekinthető-e az e-mail vagy sem, minden esetben a küldő és a címzett személyes jogait, autonómiáját és a magánszférájának a védelmét kell szem előtt tartani. Amennyiben lehetséges, a munkáltatónak tartózkodni kell a munkavállaló által elmentett – és nem azonnal törölt - e-mail-ek megtekintésétől.

c) Amennyiben a levelezés megtekintése víruskeresés miatt válik szükségessé, akkor automatikus víruskereső programot kell használni. Az így nyert információt csak az eredeti célkitűzésnek megfelelően – víruskeresésre – szabad felhasználni.

d) Amennyiben a munkavállaló távollétében szükséges a levelezési ládájának a megtekintésére, akkor gondoskodni kell arról, hogy a munkavállaló értesüljön az átvizsgálás tényéről. Az átvizsgálás csak üzleti célú lehet, rendszerint annak az ellenőrzése, hogy a munkavállaló megfelelően tartja a kapcsolatot az ügyfelekkel, megfelelő stílusban kommunikál, nem rontja a cég hitelét, stb.

e) Gondoskodni kell egy olyan programról, amely abban segít, hogy a munkavállaló saját maga is képes legyen törölni az e-mail forgalmazását.

1.2.4. A Kódex Internet használatra vonatkozó szabályai

a) A munkavállalóval pontosan kell közölni, hogy milyen feltételekkel használhatja a munkahelyi e-mail/internetet magán célra. A munkáltatónak világosan közölni kell a munkavállalóval, hogy mely internetes oldalakon és milyen információk nem kereshetők, illetve nem tölthetők le. Nem elegendő egyszerűen annak a közlése, hogy pornográf tartalmú honlapok nem látogathatók.

b) Csak kifejezetten üzleti célból lehet a munkavállaló által látogatott honlapokat vagy az általa letöltött információt ellenőrizni. Ugyanakkor a jogszerű ellenőrzés nem megfelelő, ha csak az Interneten töltött időt mérik. Ennél alaposabb kontrollra van szükség.

c) Az Internet elérés korlátozását sokkal inkább technikai eszközök (szoftverek) alkalmazásával, mint megfigyelés segítségével végezik. Például vannak olyan felismerő programok, amelyek képesek a képernyőn a bizonyos mértéket meghaladó emberi bőr felismerése esetén az elérést letiltani. Ilyen program alkalmazásával a pornográf tartalmú képek túlnyomó többsége nem tölthető le.

d) Biztosítani kell, hogy amennyiben a munkáltató engedélyezi a magán célú Internet használatot, akkor a munkavállaló privát internetes tevékenységét nem fogják megfigyelni és nem készítenek listát a meglátogatott web oldalakról.

1.3. Emberi jogi törvény (Human Rights Act, 1998)

Az Emberi Jogok Európai Konvenciójának 8. cikkelye - amely a munkavállalók védelmével foglalkozik – teljes egészében átvételre került a brit Emberi Jogi törvénybe. A törvény biztosítja a privát és a családi élet tiszteletben tartását. Az Emberi Jogi törvény 2000 októberében lépett hatályba. A törvény filozófiája alapvetően az Európai Emberi Jogi Bíróság Halford v. United Kingdom (1999) ítéletét tükrözi. Az esetben a munkavállaló a munkáltató kifejezett beleegyezésével magáncélra is használhatta a munkahelyi telefont. Ilyen esetben a munkáltató nem hallgathatja le és nem figyelheti semmilyen

eszközzel a munkavállaló telefonjait. Kivételt képez, ha a munkáltató az érintett munkavállalónak előre bejelenti a megfigyelést.

1.3.1. Szankciók

Amikor a munkáltató fegyelmi büntetésben kívánja részesíteni valamely munkavállalóját a helytelen e-mail/internet használat miatt, akkor a saját fegyelmi eljárásra vonatkozó szabályait kell alkalmaznia. Ezt írásba kell foglalni és gondoskodni kell arról is, hogy a munkavállalók mindegyike megismerhesse.

Amennyiben ezen ok miatt a munkáltató meg akarja szünteti a jogviszonyt, akkor arra kell figyelni, hogy az csak jogszerűen történhet. Ilyen esetben a bizonyítási teher a munkáltatót terheli.

A nem megengedett e-mail/Internet használat esetén a munkáltató élhet a rendes vagy rendkívüli felmondás jogával. Ilyenkor a felmondás indoka a munkavállaló képességeivel, de még inkább a magatartásával hozható összefüggésbe. Ugyanakkor a bírói gyakorlatot (tribunal) is figyelembe kell venni. A bírói gyakorlatban kialakult az a felfogás, hogy a munkavállaló jogviszonyának a megszüntetése – általában – nem lesz jogszerű, ha már az első kötelezettségszegést követően meg akarják szüntetni a munkaviszonyát.

A munkáltatónak minden esetben nagyon világos és egyértelmű bizonyítékokra kell alapoznia a jogviszony megszüntetését: a) szerződésszegés vagy b) valamilyen speciális jogszabály. Az alábbiakban ez utóbbit részletezzük.

1.4. Diszkriminációról szóló törvények (Discrimination Acts, 1975)

Általában az interneten vagy e-mail-ben küldött a szexis viccek vagy szexuális tartalmú képek legtöbb esetben alkalmasak arra, hogy a szexuális zaklatást megvalósítsák. A nemen, fajon és fogyatékosságon alapuló zaklatás ellenkezik a Nemi Diszkriminációról rendelkező törvénnyel (Sex Discrimination Act, 1975), a Faji kapcsolatok törvényével (Race Relations Act, 1976) és a Fogyatékossági Alapon történő Diszkriminációról szóló törvénnyel (Disability Discrimination Act, 1995). Ilyen esetekben fennáll a munkáltató másodlagos felelőssége a munkavállaló által elkövetett magatartásért. Az obszcénnek nem minősülő kép vagy írás is lehet offenzív és zaklató a másik munkavállaló számára. Hasonló filozófia és jogi eljárás követendő a faji vagy fogyatékosságon alapuló zaklatás esetén.

1.5. A Zaklatás elleni védelemről szóló törvény (Protection from Harassment Act, 1997)

A törvény szerint más személy zaklatása akkor lesz jogellenes, ha a zaklató felismeri vagy fel kellene ismernie, hogy magatartása egy másik személy számára nemkívánatos. A zaklatás bűncselekménynek minősül, amelynek büntetési tétele maximum 6 hónapig tartó szabadságvesztés vagy pénzbírság. A magatartás alapján magánjogi kártérítési kereset is indítható.

1.6. A szerzői jogi, design és szabadalmi törvény (Copyright, Designs and Patents Act, 1998)

Az internetről letöltött adatok, képek, stb. szerzői jogi védelem alatt állnak. A szerzői jogok megsértése kártérítési igényt von maga után. A munkavégzéshez kapcsolódó anyagok jogellenes letöltése esetén a munkáltató felel a szerzői jogok megsértéséért.

1.7. Az obszcén kiadványokról szóló törvény (Obscene Publications Act, 1959)

A számítógépes (internetes) anyagok is a törvény hatálya alá tartoznak. Amennyiben ilyen tárgyú anyagot publikálnak, az büntetőjogi jogkövetkezménnyel jár. Van egy külön ún. „obszcén teszt". Egy számítógépes rendszer adatállománya akkor minősül jogellenes tartalmúnak, ha azon olyan cikk is található, amely az obszcén teszt szűrőjén nem ment át.

A törvény értelmében a publikációt széles értelemben kell értelmezni. Magában foglalja a terjesztést, körbeküldést, eladást, odaadást, kölcsönzést, vételre való ajánlást és lízinget. A honlapon vagy belső internetes lapon közzétett információ ugyancsak publikációnak minősül és a törvény hatálya alá tartozik. Ilyen esetben az a személy lesz a publikáló, aki az adott információt a honlapra feltette.

1.8. A Büntető törvénykönyvvel módosított Gyermekvédelmi törvény (Protection of Children Act, 1978 as amended by the Criminal Justice Act, 1988)

Az egyesített két törvény értelmében a 16 éven aluli gyermekekről készített bárminemű fénykép, másolat, fax, digitális image, etc. Birtoklása és terjesztése bűncselekménynek minősül.

1.9. Telekommunikációról szóló törvény (Telecommunications Act, 1984)

A törvény 43. szakasza értelmében bűncselekménynek minősül az egyik számítógépről a másikra történő obszcén vagy egyéb módon sértő tartalmú adat – munkahelyen kívüli (közcélú) telekommunikációs rendszeren keresztül – továbbítása. Ez a jogszabályhely természetesen csak a munkáltatón kívüli (nem intranet, hanem Internet) rendszerekre vonatkozik. Meg kell jegyezni, hogy a törvény szabályai szerint, például, ha egy multinacionális vállalaton (GB-USA) belül a brit vállalatnál dolgozó munkavállaló küldd el egy üzenetet az USA-beli iroda dolgozójának, akkor ez külső kommunikációnak minősül, hiszen a két ország közötti kapcsolat megteremtése ún. közcélú (public) hálózaton keresztül történik. Még akkor is külső kapcsolatnak kell ezt tekinteni, ha a két munkavállaló ugyanannál a cégnél áll alkalmazásban.

1.10. Az engedély nélküli számítógép-használatról szóló törvény (Computer Misuse Act, 1990)

Bűncselekménynek minősül, ha engedéllyel nem rendelkező személy, szándékosan nyúl valamely számítógépes programhoz vagy adathoz, vagy ez a személy szándékosan átírja a programot, illetve módosítja a számítógépben lévő adatokat.

3. Az ellenőrzés technikai mikéntje

A munkáltatónak számos olyan lehetőség áll a rendelkezésére, amelyek segítségével képes ellenőrizni az e-mail/Internet magáncélú vagy üzleti célú használatát. A leginkább előforduló esetek a következők:

a) Biztonság

A munkáltatónak meg kell győződnie arról, hogy az általa használt rendszer megfelelő biztonsági elemekkel rendelkezik. Például, az internethez jutás csak meghatározott személyi kör számára engedélyezett. Csak nekik van személyi kódjuk a belépéshez. Bizonyos honlapokra tilos a belépés. A munkavállalóknak kizárólagosan használt saját (egyéni) azonosító kódjuk van. Ezzel jelentős mértékben elkerülhető, hogy a munkavállaló gépéről, a saját nevükben más használja a levelezést vagy az internetet.

b) Körültekintő munkaerőfelvétel és alapos képzés

A képzésnek az Internet használatán kívül elsősorban a médiák körültekintő használatára kell megtanítani a munkavállalókat.

c) Megfelelő írott szabályzatok, szerződések

Minden munkáltatónak készíteni kell egy e-mail/Internet szabályzatot. Ebben világosan le kell írni, hogy az e-mail/Internet használata során mi a kívánatos és mi a tiltott munkavállalói magatartás. A szabályzatba bele kell foglalni a fegyelmi büntetéseket és jogellenes magatartást tanúsító munkavállalóval szemben követendő eljárási szabályokat. A szabályzat egy nagyon fontos keretet teremt mind a munkáltató, mind pedig a munkavállaló számára.

d) Megfigyelés

A modern számítógépes programok képesek megfigyelni és rögzíteni a munkavállaló minden egyes mozgását az interneten, illetve az e-mail alkalmazása során. A munkáltató pedig szeretné ezeket az információkat felhasználni. A felhasználás során fokozottan figyelni kell arra, hogy nem szabad megsérteni a Lawful Business Practice Regulations előírásait.

e) Fegyelmi jellegű büntetések

Nem elég, ha a munkáltatónak van egy jó szabályzata és eljárási rendje. Neki minden esetben aktívan fel kell lépni, ha az e-mail/Internet használat során gondatlanságot vagy meg nem engedett használatot tapasztal.

Jelenleg Nagy-Britanniában nincs olyan jogszabály, amely előírná, hogy a szociális partnereknek egyeztetni kellene az e-mail/Internet használatról. Ellenben, több esetben magától a munkavállalótól kell beszerezni a hozzájáruló nyilatkozatát.

Az Információs Biztos kibocsátott egy „Gyakorlati kódexet" (Code of Practice) tervezetet a szociális partnerek közötti konzultáció lefolytatásának elősegítésére. Ez a Kó-

dex a törvény előírásait és kívánalmait próbálja átültetni a gyakorlat számára: hogyan lehet jogszerűen lefolytatni a munkahelyi ellenőrzést és megfigyelést.[65]

Franciaország

1. A munkáltató ellenőrzési joga

A munkáltató utasítási jogára vonatkozó szabályokat a francia Munka törvénykönyvének a 122-140. szakaszai szabályozzák. A Dujardin v Instinet France esetben a francia Legfelsőbb Bíróság kimondta, hogy a „munkáltatónak joga van ahhoz, hogy munkaidőben a munkavállalók munkavégzését megfigyelje és ellenőrizze." Egyedül a rejtett megfigyelés tiltott.

1.1. A munkáltató ellenőrzési jogának határai és akadályai

A bizonyítékok beszerzésével kapcsolatos nehézségek. Számos bírósági ítéletből kiolvasható, hogy milyen nehéz feladat a munkáltató számára elfogadható bizonyítékot találni arra nézve, hogy a munkavállaló nem megfelelően használja a munkáltató eszközeit (beleértve az e-mail/Internet-et is). Álljon itt érzékeltetésül néhány eset.

a) A munkáltató azért bocsátotta el a munkavállalót, mert a munkahelyi számítógépének az ellenőrzésekor – ahol a munkavállaló nem volt személyesen jelen – olyan file-t is találtak a gépen, amelyek nem kapcsolódtak a munkavállaló munkakörében leírt tevékenységéhez. A bíróság jogszerűtlennek minősítette a felmondást. Indokai között előadta, hogy a munkáltató – mivel a munkavállaló nem volt jelen – nagyon könnyen másolhat fel a munkavállaló gépére – annak beleegyezése és tudomása nélkül – olyan file-t, ami kompromittálhatja a munkavállalót. A munkáltatónak nem volt bizonyítéka arra nézve, hogy a kifogásolt file-t tényleg a munkavállalóé.[66]

b) Egy másik esetben a bíró jogszerűtlennek minősítette a munkáltató döntését (munkaviszony megszüntetése), amikor a munkavállaló munkaidő alatt magán célra (pornográf képeket nézegetett) használta a munkahelyi számítógépet. A bíróság nem fogadta el a munkáltató által bizonyítékként bemutatott merevlemezt. Azt kifogásolták, hogy a merevlemezen nem volt olyan biztonsági csík, amely azt mutatná, hogy a lemez érintetlen. Ennek hiányában a bíróság azt mondta, hogy egy ilyen lemezt nagyon könnyű manipulálni, következésképpen ebben a formájában nem fogadta el bizonyítékként. Ezért a bíróság a benyújtott bizonyíték alapján a munkaviszony megszüntetését nem találta megalapozottnak.[67]

A fenti jogesetektől elvonatkoztatva megállapítható, hogy a munkáltató által a munkavállaló rendelkezésére bocsátott számítógépes eszközök és programok rendeltetésellenes használatáért a munkáltató jogszerűen alkalmazhat fegyelmi büntetést, sőt meg is szüntetheti a jogviszonyt. A munkavállaló jogsértő magatartásának a bizonyítása nagyon nehéz feladat, ezért azt nagyon körültekintően kell végezni. Például, a számítógépet a

[65] I. m. pp. 34–35.
[66] Court of Appeals of Rouen, 14 may 1996, SARL Médical Informatique v. Dedieu.
[67] Labour Court Nanterre, 16 July 1999, Mr. R. v. IBM France.

munkavállaló jelenlétében kell ellenőrizni, vagy maga a munkavállaló kéri, hogy a munkáltató ellenőrizze a gépét stb.

2000. március 13-án elfogadták az elektronikus aláírásról rendelkező törvényt. A fent idézett jogesetek ezzel a törvénnyel összhangban állnak. A törvény kimondja, hogy az elektronikus dokumentumoknak a bizonyítás és a hitelesség szempontjából éppen olyan erejük van, mint a hagyományos formában készült írott dokumentumoknak, feltéve, ha a szerző pontosan meghatározható.

1.2. A munkavállalók alapvető joga a magánszféra védelmére

A francia Polgári törvénykönyv 9. cikkelye garantálja, hogy minden személy magánéletét tiszteletben kell tartani. Ez a jogszabály vonatkozik a munkavállaló személyre is. A védelem a munkavégzés egész tartamára kiterjed.

A Munka törvénykönyvének 120-2. cikkelye kimondja, hogy „senki, semmilyen módon nem korlátozhatja az egyének személyiségi jogait, és az egyéni, illetve a kollektív szabadságjogaikat, kivéve ha a korlátozást az elvégzendő feladat természete igazolja vagy a korlátozás arányos az elérendő céllal."

Ha a munkáltató tudja is igazolni, hogy az általa gyakorolt kontrol az elérendő célkitűzéssel arányos és igazolható, még akkor sincs joga arra, hogy a munkavállaló magánlevelezését elolvassa vagy megnézze.

A kommunikációs titokról (secrecy of communication) rendelkező törvény (1991) előírja, hogy a munkáltató fő szabály szerint nem férhet hozzá a munkavállalói magáncélú kommunikációjához. Kivételt képez ez alól a tilalom alól, ha erre jogszabály vagy hatósági határozat kötelezi, illetve amikor jóhiszeműen eljárva cselekszik. Az utóbbi kitételt (jóhiszeműség) a francia adatvédelmi hivatal (CNIL) a következőképpen értelmezte: a jóhiszeműség keretei közé még belefér, ha a munkáltató vagy megbízottja az elektronikus levelezés gyakoriságát, a küldött levelek hosszát és a csatolt file-ok terjedelmét vizsgálják. Ugyanakkor nem fér bele a megengedett határok közé, ha a levelezés tartalmába is beleolvasnak.[68]

A Büntető törvénykönyv 226-15. cikkelye büntetni rendeli a magánlevelezés titkosságának a megsértését. A Btk. tényállása kiterjed mind a hagyományos úton küldött postai levélre, mind pedig már az elektronikus úton küldött információkra, beleértve az intranet és az Internet rendszereket is.

A Versailles-i Fellebbviteli Bíróság az egyik ítéletében[69] kimondta, hogy a munkáltató nem tudta bizonyítani – a munkavállaló által a munkáltató számítógépén és rendszerén keresztül küldött magán e-mail tartalmának a bemutatásával –, hogy a munkavállalója nem teljesítette a munkaviszonyból származó köztelezettségét. A bíróság rámutatott, hogy a levélnek volt egy pontosan meghatározható feladója (a munkavállaló) és volt egy pontosan megnevezett magánszemély címzettje. Következésképpen ez a levél magánjellegű levélnek minősül. A magánlevelezés titkosságát pedig védi a jog. Ezért a munkáltató bizonyítéka nem volt felhasználható a bíróság előtt. Következésképpen a munkáltató nem használhatja fel az abban található információkat.

---

[68] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 30–31.

[69] M. Venet v. S.A. France Réseaux Systemes, June 21, 2001.

Ezt a logikát erősítette meg a Legfelsőbb Bíróság Szociális Tanácsa által 2001. október 2-án hozott ítélet. A konkrét ügyben a munkavállaló a munkáltató (Nikon France) határozott és egyértelmű tiltása ellenére magánjellegű e-mail-t küldött a munkahelyi számítógépéről. A munkáltató ezért elbocsátotta a munkavállalót. Az ítélet vesztese a Nikon France lett. A bíróság kimondta, hogy a munkavállalónak, mint természetes személynek joga van a munkavégzés közben is ahhoz, hogy az alapvető szabadságjogait és a magánszféráját tiszteletben tartsák. Ennek értelmében a munkáltató a munkavállaló által, a munkahelyen és a munkáltató eszközeivel küldött elektronikus levelek esetén is köteles tiszteletben tartani a munkavállalók személyiségi jogait, tehát a konkrét esetnél maradva nem olvashatja el a munkavállaló magánleveleit. Ez a kötelezettség tehát akkor is terheli, ha a munkavállaló a munkáltató eszközeit használva bonyolította le a magánjellegű levelezését, továbbá akkor is, ha kifejezetten megtiltotta a munkavállalónak a munkavégzés időtartama alatti személyes célú e-mail/Internet használatot.

A bíróság még kifejtette azon álláspontját is, hogy a napi szokásos mennyiségű e-mail/Internet használatot meg kellene engedni a munkavállalóknak, mivel ez alapvetően nem érinti hátrányosan a napi munkavégzést. Ugyancsak javasolta még a bíróság, hogy a küldött e-mail-ek jól látható részén minden esetben fel kellene tüntetni, hogy hivatalos vagy magánlevélről van szó. Természetesen ezzel az állásponttal nem mindenki ért egyet.

Annak a munkáltatónak megállapítható a felelőssége, aki megnyitja, elolvassa, eltéríti vagy kitörli a munkavállaló elektronikus postaládájában lévő, vagy azon keresztül menő elektronikus leveleit. A felelőssége egyrészt magánjogi felelősség. A Munka törvénykönyvének 120-2 cikkelye alapján köteles megtéríteni a magatartásával okozott kárt (magánjogi kártérítés). Ezen túlmenően büntetőjogi felelősséggel is tartozik, mivel szándékosan megsértette a levéltitkot (Büntető törvénykönyv 226-15. cikkely). A bűncselekmény büntetési tétele maximum 1 év és/vagy pénzbüntetés.

A gyakorlatban sokszor előfordul, hogy a munkáltató szándékosan, az érintett személy tudta nélkül hatol be a munkavállaló elektronikus postaládájába, rendszerint azzal a céllal, hogy az ott talált információkat a saját javára és a munkavállaló ellen fordíthassa. A bírói gyakorlat szerint a munkáltató magatartása akkor is tisztességtelen és jogellenes, ha a munkavállaló saját titkos kódjával lépett be a rendszerbe.

A Legfelsőbb Bíróság Büntetőjogi Kollégiuma nem osztotta a Szociális Jogi kollégium álláspontját. Egy 1992. január 6-án kelt ítéletben kimondták, hogy amennyiben joggal hihető, hogy a vizsgált levelezés hivatali levelezés, ilyenkor a munkáltatói beavatkozás felróhatósága nem áll meg, következésképpen nem lehet bűncselekményről beszélni. A konkrét esetben az egyik kutatóintézetben (French National Institute of Reserach, CNRS) dolgozó munkatárs felettese felnyitott három olyan levelet, amelyet a kutatónak címeztek. A levélen olvasható volt a kutatóintézet és a címzett neve, valamint a kutatóintézet címe. Semmi nem utalt arra, hogy magánjellegű levelekről van szó. Ezekre a körülményekre tekintettel nem állapították meg a munkáltató büntető jogi felelősségét.

2. Szankciók

2.1. A helytelen e-mail/Internet használat során kiszabható munkáltatói büntetések

A francia bírói jogban általánosan kialakult az az álláspont, hogy amennyiben a munkavállaló a munkáltató telephelyén, a munkáltató eszközeivel, a munkáltató kifejezett és világos tiltása ellenére magánjellegű levelezést folytat, vele szemben jogszerűen szabható ki fegyelmi büntetés, vagy rendkívüli felmondással elbocsátható, feltéve, ha a levél tartalma a munkáltatóra nézve offenzív tartalmú.

Például, a munkáltató jogszerűen bocsátotta el azt a munkavállalóját, aki havonta 11 órán keresztül saját (magán) célra használta a munkahelyi telefont. A bíróság megjegyzései a következők voltak: *a)* a munkáltató minden egyes munkavállalójával tudatta, hogy a kommunikációs rendszerbe olyan eszközt szereltek be, amely számlálja és rögzíti a munkahelyen folytatott telefonbeszélgetéseket; *b)* a rendszer telepítésére hatósági engedéllyel (National Commission of Data Processing and Liberties) rendelkeztek és *c)* a telefonellenőrzés tisztességes és megfelelő garanciákat tartalmazó módszerrel került lebonyolításra.[70] A szerző álláspontja szerint a telefonhívásra alapozott ítélet a munkáltató által fenntartott e-mail/Internet rendszerekre is analógia módjára alkalmazható.

2.2. A bizalmas (titkos) munkáltatói információk védelme

Eddig egyetlen ítélet[71] született ebben a témakörben. A bíróság ítélete szerint a munkáltató jogszerűen büntette meg azt a munkavállalóját, aki egy e-mail-t küldött a korábbi kollégájának, amelyben informálta őt a munkáltató által tervezett szervezeti átalakításról. A munkáltató megnézte a munkavállaló elektronikus levelesládáját és abban megtalálta a levelet, majd fegyelmi eljárást indított a munkavállalóval szemben. (Zárójelben jegyezzük meg, hogy a munkavállalók magánszférájának védelméről szóló törvény (ld. fent) előírásai szerint a munkáltató nem nézheti meg jogszerűen a munkavállaló levelesládáját. Ennek a munkáltatói magatartásnak a jogszerűsége tehát megkérdőjelezhető.)

3. Az ellenőrzés technikai módszerei

3.1. Az e-mail/Internet használat szervezeti rendszere

A munkáltatónak számos olyan technikai lehetősége van, amely segítségével ellenőrizheti a munkavállaló munkahelyi e-mail/Internet használatát. (Például a munkáltató képes ellenőrizni a munkavállaló által ledolgozott munkaidő hosszát, azzal a módszerrel, hogy megvizsgálja a munkavállaló számítógépe milyen hosszan volt rákapcsolva a központi terminálra. Képes ellenőrizni, hogy a munkavállaló milyen internetes kapcsolatokat létesített és milyen dokumentumokat nyitott meg stb.)

A munkáltató csak olyan ellenőrzési módszereket alkalmazhat, amelyek jogszerűek és csak olyan adatokat használhat fel, amelyeket számára a jogszabály megenged. A vonatkozó jogszabályok értelmében a munkáltató ellenőrzésének a következő feltételeknek kell megfelelnie:

[70] Court of Versailles, 28 November 1995.

[71] Court of Montbéliard, 19 September, 2000. Madeleine R. v. Sulzer Orthopédie Cédior.

a) Előzetes konzultáció a munkavállalói érdekképviseleti szervezettel

Amennyiben a munkavállalók létszáma eléri az 50 főt, akkor az alkalmazni kívánt ellenőrzési módszerről a munkáltatónak előzetesen (a rendszer felszerelése előtt) konzultálni kell az üzemi tanáccsal (Comité d'entreprise).[72] Ez a feltétel nem vonatkozik az 50 fő alatti munkáltatókra.

b) A munkavállalók előzetes informálása

A Munka törvénykönyvének L 121-8. cikkelye kimondja, hogy „semminemű személyre (munkavállalóra) vonatkozó információ nem gyűjthető be olyan módszerrel, amelyről a munkavállalót előzetesen nem értesítették". Ennek értelmében a munkáltatónak előre kell értesíteni a munkavállalót, hogy milyen módszerrel vagy eszközzel végzi az intranet/Internet ellenőrzését.

A bírósági gyakorlat szerint a munkavállaló előzetes értesítése előfeltétele annak, hogy a végzett megfigyelés jogszerű legyen, illetve az ellenőrzés során beszerzett adatokat jogszerűen fel lehessen használni.

A Neocel esetben [Cass. Soc. 20/11/91 RDS 1992(2), 77] a bíróság kimondta, hogy a Polgári törvénykönyv értelmében a munkavállaló titkos megfigyelése tilos.

c) Az Adatvédelmi hatóság („C.N.I.L.") előzetes értesítése

Az 1978. január 6.-án kiadott törvény értelmében, ha a munkáltató által telepített megfigyelési rendszer konkrét személyre szóló információkat gyűjt, akkor a munkáltatónak egy előzetes bejelentést kell küldeni a National Commission of Data Processing and Liberties („C.N.I.L.") hivatalhoz. Amennyiben elmulasztja a bejelentést, akkor bűncselekményt követ el. Ilyen esetben is szükséges a munkavállaló beleegyezése. Ezen kívül a munkavállalót megilleti a jog, hogy az összegyűjtött adatot megnézhesse, javíthassa és kérje a kifogásolt adat törlését. Erre a külön bejelentési eljárásra azért van szükség, mert ellenkezik az általános gyakorlattal, mely szerint a munkáltató csak név nélkül gyűjthet adatokat.

d) E-mail/Internet használatra vonatkozó belső munkahelyi szabályzat

A közelmúlt francia bírói gyakorlatában rejlő jogalkalmazási bizonytalanságok elkerülése érdekében ajánlatos a munkáltatóknak megalkotniuk a munkahelyi e-mail/Internet használatra vonatkozó szabályzatukat. A szabályzatban a munkahelyi elektronikus eszközök használatára vonatkozó szabályokon kívül rögzíteni kell a munkavállaló felelősségére vonatkozó szabályokat és a rendeltetésellenes használat esetén a vele szemben alkalmazható szankciókat.

A munkahelyi szabályzatra a fent vázolt formai követelmények vonatkoznak. (Konzultáció a munkavállalói érdekképviselettel stb.) Továbbá, ha a belső szabályzat általános szabályokat és fegyelmi büntetéseket is tartalmaz, akkor – az üzemi tanács döntésével együtt – be kell nyújtani a Munkaügyi Bírósághoz, valamint a helyben szokásos módon ki kell függeszteni a munkahelyen és el kell küldeni a munkaügyi felügyelőségre.

[72] Munka törvénykönyve L. 432-2-1. §.

A munkáltató kötelessége, hogy minden egyes munkavállaló megismerhesse a belső szabályzatot. Ezért a szabályzat egy példányát minden munkavállalónak személyesen át kell adni vagy ajánlott levélben el kell küldeni azt. A munkavállaló írásban köteles nyilatkozni arról, hogy a szabályzatban foglaltakat megértette. A nyilatkozattétellel egyidejűleg igazolja a szabályzat átvételét.

A megalkotott, majd kézbesített és tartalmában a munkavállalók által megismert szabályzat lehetővé teszi, hogy egy ellenőrzést követően, ahol fény derül a szabályellenes elektronikus média használatra munkáltatónak joga legyen a fegyelmi büntetés (ezek közül akár a legszigorúbb, az elbocsátás) kiszabására is.

Ugyanakkor nagyon fontos, hogy amennyiben a munkáltatónak valamilyen oknál fogva be kell lépnie a munkavállaló elektronikus levelesládájába, akkor nagyon körültekintőnek kell lennie. A belépésre csak úgy kerülhet sor, hogy nem nyithatja meg, nem olvashatja, változtathatja meg vagy törölheti a munkavállaló meglévő üzeneteit. Az indokolatlan belépés büntető és magánjogi jogkövetkezményeket vonhat maga után.

Egy fontos bizonyítással kapcsolatos kérdés. A jelenlegi bírói gyakorlat álláspontja szerint a vonatkozó jogszabályok és a munkaszerződés nem teszi lehetővé a munkáltató számára, hogy a munkajogi perben (pl. jogviszony megszüntetése vagy fegyelmi büntetés kiszabása esetén) a munkavállaló magánjellegű levelezéséből származó információkat terjesszen bizonyítékként a bíróság elé. A munkáltató a munkahelyen lebonyolított magáncélú levelezés tartalmát még akkor sem használhatja fel bizonyítékként a bírósági eljárásban, ha egyébként az a birtokában van. Csak magát a jogellenes használatot, vagy a magáncélú használat tartamát, a meglátogatott vagy megnyitott honlapok címét használhatja fel bizonyítékként.

Dánia

Dániában a munkahelyi elektronikus megfigyelést és ellenőrzést leginkább kollektív szerződésben, azon belül is az ún. kollektív alapszerződésekben (basic agreement) szabályozzák. A megállapodások központi eleme annak a rögzítése, hogy a munkáltatónak joga van a munkahelyen folyó munka ellenőrzésére. A bírói esetjog kimondta, hogy a munkáltatónak ez a joga nem abszolút. A munkáltató akkor jár el jogszerűen, ha az ellenőrzéshez való jogát rendeltetésszerűen gyakorolja és nem sérti ezzel a munkavállalók alapvető emberi jogait.

A Dán Munkáltatói Érdekképviseletek (Danish Confederation of Employers) és a Dán Szakszervezeti Szövetség (Danish Confederation of Trade Unions) között létrejött alap kollektív szerződés (2001. április 24.) függeléke tartalmazza, hogy a munkáltató bármilyen megfigyelési tevékenységről két héttel az elkezdés előtt köteles tájékoztatni a munkavállalókat.

A dán Büntető törvénykönyv 263. cikkely (1) és (3) bekezdései szerint a telekommunikáció megfigyelése és ellenőrzése jogellenes. Függetlenül attól a ténytől, hogy a kommunikáció magán- vagy üzleti jellegű. Nem teljesen egyértelmű, hogy a Büntető törvénykönyv idézett rendelkezése vajon alkalmazható-e az e-mail és az Internet kommunikációra.

A Dán Adatvédelmi Hivatal (Danish Data Protection Agency) néhány döntésében kimondta, hogy a munkáltatónak joga van a munkavállaló Internet-forgalmának a rögzítésére. Ugyanakkor erre csak akkor kerülhet sor, ha az alábbi feltételek fennállnak.

a) A megfigyeléshez és az adatok rögzítéséhez a munkáltatónak jogos gazdasági érdeke fűződik. A döntés külön rendelkezik az érdekkonfliktusról, amikor kimondja, hogy a munkáltató érdeke csak akkor lesz jogszer, ha a munkavállaló alapvető jogai nem haladják azt meg. Másképpen fogalmazva, ha a munkavállaló valamely alapvető emberi jogát (pl. magánszféra védelme) sérti a munkáltató megfigyelése és adatrögzítése, akkor a munkáltatói magatartás nem lehet jogszerű, még akkor sem, ha az sem vitatható, hogy a munkáltatói döntés mögött is jogos gazdasági érdek húzódik meg. Az elv védi a rendszerint gyengébb és kiszolgáltatottabb helyzetben lévő munkavállaló érdekeit.

b) A munkáltatónak előre és egyértelműen kell informálnia a munkavállalót a tervezett megfigyelésről. Az ellenőrzés mögött annak az alapos feltételezésnek kell meghúzódnia, hogy a munkavállaló nem a megengedett célra használja a munkahelyi elektronikus kommunikációs eszközöket.

A Dán Adatvédelmi Hivatal arra az álláspontja szerint a munkáltató biztonsági másolatot készíthet a munkavállaló által küldött e-mail-ről. A munkavállaló akkor nézheti meg a rögzített elektronikus levelezést, ha alapos gyanú merül fel arra nézve, hogy a munkavállaló nem a megengedett célra használta a munkahelyi e-mail rendszert. Az e-mail megfigyelés és ellenőrzés jogszerűségéhez az alábbi feltételnek kell fennállnia: A megfigyelést és az adatok rögzítését csak akkor lehet elvégezni, ha ahhoz a munkáltató jogos érdeke fűződik és a munkavállaló alapvető jogait védő érdek nem haladja meg a munkáltatói érdeket. A munkáltató jogos gazdasági érdeke lehet, például az üzleti tevékenységhez kapcsolódó érdek, biztonsági érdek, a megsérült elektronikus kommunikációs rendszer helyreállítása, dokumentálás stb.

A munkáltató a munkavállalói e-mail/Internet ellenőrzés és megfigyelés során az adatfeldolgozásra vonatkozó „jó gyakorlat" (good practice) elvárásainak megfelelően köteles eljárni.[73]

Görögország

A Görög Alkotmány [(1975), módosítva 2001. április] tartalmazza a magánszféra és a tág értelemben vett személyiség védelmére vonatkozó szabályokat. Ezen túlmenően a görögöknél alkotmányos rendelkezések írják elő az emberi értékek (human value) védelmét és tiszteletét. Erről a jogáról egyetlen személy sem mondhat le jogszerűen. A görög jog előírásainak értelmében, érvénytelen az olyan szerződés, amely kifejezetten csorbítja az emberi jogokat.

A görög Polgári törvénykönyv 178. és 179. cikkelyei kimondják, hogy bármely olyan jogi magatartás, amely a jó erkölcsbe ütközik érvénytelen. Ugyancsak érvénytelen minden olyan magatartás, amely mások emberi jogát, szabadságjogát sérti, illetve korlátozza. Az alkotmányban védett emberi jogok, illetve szabadságjogok közé sorolják a magánszféra védelmét (right to privacy) is.

A fent idézett alkotmányos rendelkezések alapján a munkáltató jogszerűen nem ellenőrizheti, illetve nem figyelheti meg a munkavállaló munkahelyen történő elektronikus levelezését. Az ilyen munkáltatói magatartás ellenkezik az alkotmányban rögzített ma-

[73] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 28.

gánszféra védelméhez való joggal, amely a munkavállalót, mint személyt egyaránt megilleti.

A 1767/1988-as törvény (módosította a 2224/1994. törvény) kimondja, hogy az üzemi tanácsnak meghatározott kérdésekben együttdöntési joga van. Ehhez a körhöz tartozik a munkavállalók ellenőrzése és megfigyelése is.

A Görög Adatvédelemi Hivatal (Hellenic Data Protection Authority) már hozott döntést[74] munkahelyi megfigyelési ügyben.[75]

Spanyolország

A Spanyol Alkotmány 18. cikkelye rendelkezik a magánjellegű kommunikáció titokvédelméről. Az alkotmány cikkelyét alkalmazni kell mind a hagyományos kommunikációra (postai levél), mind pedig a telekommunikációs eszközökre, de a hozzá fűzött kommentár ezekből csak a telegráfot és a telefont említi. Ennél modernebb eszközökre nem történik konkrét utalás.

Külön jogszabály vonatkozik a jogszerű adatfeldolgozásra. Ez a jogszabály korlátozza a jogszerű adatfeldolgozást. A korlátozás indoka a személy és a család magánszférájának és méltóságának a védelme. A jogalkotó azon az álláspontón van, hogy amennyiben az állampolgárok ezen alapvető jogai sérülnek, akkor nem gyakorolhatják szabadon az egyéb jogaikat sem.

A Munka törvénykönyv 5. cikkelye kimondja, hogy a munkavállaló legfontosabb feladata, hogy a munkaviszonyból eredő kötelezettségeit legjobb tudása szerint és jóhiszeműen eljárva teljesítse. A ettől eltérő magatartása szerződéses kötelezettségszegést valósít meg (Spanyol Mt. 54.2. cikkely).

A Munka törvénykönyvének 18. cikkelye kimondja, hogy „a munkavállalót, illetve öltözőszekrényét és egyéb személyes tárgyát csak abban az esetben lehet átkutatni, amikor *a)* ez a munkáltató vagyontárgyainak a megóvása miatt szükséges, vagy *b)* a munkatársak nyugalmának a megőrzése miatt kívánatos. A fenti feltételek fennállása esetén is a kutatást, illetve átvizsgálást csak munkaidőben és a munkahelyen lehet elvégezni. Minden esetben a munkavállalói érdekképviselet arra feljogosított képviselője vagy ha ilyen személy akadályoztatva van, akkor valamely munkatárs jelenlétében lehet elvégezni. Ilyen munkáltatói cselekmények során is a munkáltató köteles tiszteletben tartani a munkavállalók méltóságát és személyes jogait.

A Munka törvénykönyvének a 20. cikkelye a munkáltató irányítási, utasítási, szervezési és ellenőrzési jogairól rendelkezik. A munkáltató minden megfelelő eszközt alkalmazhat a munkavállalók tevékenységének az ellenőrzésére és értékelésére. Általános szabály, hogy ilyenkor is tiszteletben kell tartani a munkavállalók emberi méltóságát.

A Munkabiztonságról rendelkező törvény (Labour Hazards Prevention Act, 1995) előírja, hogy a munkáltatónak előzetesen konzultálnia kell a munkavállalókkal a munkabiztonsággal kapcsolatos intézkedések bevezetése előtt. Ebbe beleértendő a tervezés, a munkaszervezés, új technológiák bevezetése és minden olyan intézkedés, amely a munkavállalók munkahelyi egészségét és biztonságát érinti.

[74] A döntés – sajnos – jelenleg számunkra nem elérhető.

[75] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 29.

A Munka törvénykönyve és a Szakszervezeti törvény (Union Freedom Act, 1985) szabályozása egymással összhangban kívánja megteremteni a munkavállalói érdekek képviseletét a munkáltató döntéshozatali mechanizmusában. Ezt a kollektív érdekérvényesítő testület (Personnel Delegates és Company Committees) –a magyar munkajogban ez az üzemi tanács fogalmához hasonlít leginkább – és a szakszervezeti képviselő révén kívánja megvalósítani.

A Polgári törvénykönyv 1903. cikkelye kimondja, hogy alapvetően a munkáltató felel a munkavállalója által – munkaviszonyából eredő kötelezettségei teljesítése során – harmadik személy részére okozott károkért.

A Büntető törvénykönyv 197. cikkelye büntetni rendeli azt a magatartást, amikor azzal a szándékkal birtokolják valaki más személyes levelét, hogy az abban rejlő személyes titkot vagy a levél címzettjének a magánszféráját érintő információkat kifürkészszék.[76]

Írország

Az ír Alkotmány 40.3.1. cikkelye garantálja, hogy az állam a törvényhozásával – az ésszerűség határain belül maradva – védi és tiszteletben tartja az állampolgárok személyhez fűződő jogait. Ezek a személyiséghez fűződő alapvető állampolgári jogok nem „mérhető" jogok (unnumerated rights). Ezt az álláspontot az ír bírói gyakorlat is megerősíti. Az utóbbi időben az ír esetjog is elismerte a magánszféra védelmét, mint az állampolgárok egyik személyhez fűződő jogát.[77]

Olaszország

Az olasz alkotmány 15. cikkelye garantálja levelezés és minden más kommunikációs forma szabadságát és titkosságát.

Az olasz jog előírásai szerint a munkavállaló elektronikus levelezését más személy (pl. munkáltató) csak jogszabályi felhatalmazás alapján tekintheti meg.

Az olasz Adatvédelmi Hatóság álláspontja szerint a fenti jogszabályhelyeken előírtakat kell alkalmazni a munkavállaló e-mail forgalmának a megfigyelésére is. Egy 1999. július 12-én kelt Véleményükben (Opinion) kimondták, hogy személyiségi jogi szempontból az elektronikus levelezést ugyanúgy kell tekinteni, mint a hagyományos levelezést. Ugyanezt a felfogást tükrözi az 1993. évi 547. számú törvény, amely a számítógépes bűncselekményekről rendelkezik. Az 1997. évi 513. számú rendelet kimondja, hogy az elektronikus dokumentumokat – beleértve az elektronikus levelezést is – ugyanolyan védelemben kell részesíteni, mint a tradicionális levelezést.

Az Adatvédelmi Hivatal fent idézett Véleménye (Opinion) kimondja még, hogy a zárt körű csoporton belül (restricted access newsgroup) vagy zárt levelezési listán lévő személyek között, a munkáltató elektronikus eszközeinek használatával küldött levelezést magánjellegű kommunikációnak kell tekinteni. Az ilyen dokumentumokat a munkáltató nem ellenőrizheti, nem nyithatja meg.

[76] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 29–30.

[77] I. m. p. 31.

Az Adatvédelmi Hivatal jelenleg egy az e-mail megfigyelésre vonatkozó iránymutatás kiadására készül.

Az olasz Adatvédelmi törvény (Law No. 675/1996) 43(2) cikkelye kimondja, hogy ez a szabályozás nem érinti a munkavállalók jogairól rendelkező hatályban lévő munkajogi szabályozást (Law No. 300/1970). Az utóbbi törvény 4. cikkelye megtiltja a munkavállalók megfigyelését. Továbbá a munkavállalók megfigyelésére bármilyen formában – az indirekt módot is beleértve – alkalmas eszközök, illetve technológiák bevezetéséhez az illetékes szakszervezet beleegyezése szükséges. Az ilyen eszközök bevezetése csak akkor lehet indokolt, ha az a munkáltató működésének, a termelésnek és/vagy a munkahelyi biztonságnak a javítását szolgálja.[78]

Portugália

A portugál Alkotmány meglehetősen előremutató ebben a kérdésben. A többi ország gyakorlatától eltérően nemcsak egy általános garanciális cikkely szabályozza a személyiségi jogok és a magánszféra védelmét, hanem a 35. cikkely kifejezetten foglalkozik a számítógépes adatfeldolgozással kapcsolatban felmerülő adatvédelem problémájával. Az Alkotmány ugyancsak kimondja a magánélet intimszférájának a megőrzéséhez való jogot, valamint az emberi méltósághoz való jog védelmét (26. cikkely). Ugyancsak alkotmányos védelemben részesül a levéltitok és minden egyéb magánjellegű kommunikáció [34. cikkely (1)]. A 34. cikkely 4. bekezdése alapján tilos az állami szervek beavatkozása (kontrolja) a magánlevelezésbe, a telekommunikációba és más kommunikációba. Kivétel ez alól a szabály alól, ha a büntető eljárás keretei között jogszabály felhatalmazást ad a hatósági beavatkozásra. Az alkotmány 18. cikkelye értelmében a fent említett garantált jogokat mind a köz, mind pedig a magánszférában – beleértve a munkaviszonyt is – biztosítani kell.

Az alkotmány 54. cikkelye előírja, hogy a munkavégzés körülményeit érintő változásokról az üzemi tanácsot tájékoztatni kell és az üzemi tanácsnak ezen kérdésekben konzultációs joga van.

A Portugál Adatvédelmi Bizottság 1998-as döntésében a levelezés titkosságával foglalkozott. A döntés egy olyan üggyel kapcsolatos, amelyben egy telekommunikációs cég nem adott ki bizonyos munkavállalói információkat a bírósági megkeresésre. A Bizottság rámutatott, hogy az alkotmány 34. cikkelyének 1. és 4. bekezdései védik a levelezés titkosságához való jogot. Ez a védelem mind az adatforgalomra, mind pedig a kommunikáció tartalmára kiterjed.

A Munkaszerződésről rendelkező törvény (Labour Agreement Act) 39.1. cikkelye kimondja, hogy a munkáltató joga a munkavégzés feltételeinek a meghatározása. Ezeket a szabályokat a munkaszerződésben vagy a saját belső szabályzataiban rögzítheti. Amennyiben működik üzemi tanács a munkáltatónál, akkor ezt a szervet a munkáltató köteles előre értesíteni a szabályzat tartalmáról. Ezeket a munkáltató által alkotott szabályokat a munkaügyi felügyelőség ellenőrzi és hagyja jóvá (Munkaszerződésről rendelkező törvény 39.3 és 13. cikkelyei).

[78] I. m. p. 31.

A munkáltatónak tilos bármilyen formában és eszközökkel megakadályozni, hogy a munkavállaló az alkotmányban vagy az egyéb jogszabályokban rögzített jogait gyakorolhassa (Munkaszerződésről rendelkező törvény 21.1. cikkely).

Az 5/94. számú törvényerejű rendelet (decree-law 6/94 of 11 January) – az EU-s 91/5333/EC irányelven alapulva – kimondja, hogy a munkáltató kötelessége értesíteni a munkavállalót a munkaszerződésben foglalt vagy a munkaviszonyból eredő munkavégzési feltételekről. Ezeket az információkat írásban, a munkáltató aláírásával ellátva kell közölni (4. szakasz).[79]

Finnország

A munkáltató megfigyeléshez való joga a munkaszerződés és az új munkaszerződésről rendelkező törvény[80] figyelembe vételével határozható meg. A jogszabály nem tartalmaz erre vonatkozó részletes előírásokat. Figyelembe véve a hagyományokat, nem jogi normában szabályozott elv, hogy a megfigyelésnek korrektnek kell lenni és csak odáig terjedhet, ameddig a munkáltató objektíve igazolható érdekeit szolgálja. Mászóval nem lehet rosszhiszeműen visszaélni ezzel a lehetőséggel.

2001. október 1-én Finnországban elfogadták azt a törvényt,[81] amely a munkavállaló személyiségi jogait és magánszféráját védi a munkaviszony fennállása alatt.

A törvény bevezető rendelkezései között megemlíti, hogy a finn szabályozásnak túl kell lépnie az EU-s irányelv előírásain. A kiindulási pont az volt, hogy az általános adatvédelmi törvény nem képes teljes mértékben megfelelni a munkaerőpiac résztvevői elvárásainak. A kettő közötti kapcsolat: a munkavállalók személyiségi jogait védő törvényt kell elsősorban alkalmazni és ha az általános adatvédelmi törvénnyel konkurenciába kerülne, akkor a speciális szabály megelőzi az általános szabályt, vagyis a munkavállalók személyiségi jogait védő törvényt kell először alkalmazni. Jelenleg a finn munkavállalók személyiségi jogait védő törvény egyedülálló szabályozás az EU-ban, mivel nincs olyan másik tagállam, amelyben ilyen széles körben védenék a munkavállalók személyiségi jogait. Minden bizonnyal a jövőben a többi tagállam is követi a jó példát. Ugyanakkor azt is meg kell jegyezni, hogy a finn törvény a címében jelzett kérdéskörnél szűkebb tárgyi hatállyal bír. A törvény a következő fontosabb kérdésekről rendelkezik: a munkavállalóról történő adatgyűjtés; személyiségi és értékelési teszt; egészségügyi – beleértve alkohol és drog-vizsgálat és genetikai teszt; a munkavállalók tevékenységének technikai eszközökkel történő megfigyelése, ezen belül az e-mail és egyéb telekommunikációs eszközök használatának az ellenőrzése.

Rendeltetését tekintve ez a törvény a Személyes Adatok Védelméről rendelkező törvényt egészíti ki. A törvény rendelkezéseit mind a magán, mind pedig a közszférában alkalmazni kell. A törvény személyi hatálya a munkaviszonyban állókon kívül kiterjed még a munkára jelentkező személyekre is.

A törvény 9. cikkelye foglalkozik kifejezetten a munkavállalók megfigyelésével. A törvény célja nem a technikai ellenőrzésre és megfigyelésre vonatkozó jogok és kötelezettségek, illetve az információs hálózat használatára vonatkozó szabályok megalkotása volt, hanem olyan munkahelyi szabályzatok megalkotására való ösztönzés, amely ezzel a

[79] I. m. p. 33.

[80] 2001. évi 55. sz. törvény (2001. július 1-én lépett hatályba.).

[81] 2001. évi 477. sz. törvény (2001. október 1.).

problémával konkrétan foglalkozik és a felek legjobb akaratának megfelelően rendezi azt.

A törvény általában konkrét anyagi jogi normákat nem ír elő az egyes jogintézmények működésére nem határozza meg konkrétan, hogy a munkáltató mit tehet és mit nem, stb. A törvényben szereplő szabályok sokkal inkább a munkáltató elvárható és megengedhető viselkedését behatároló minőségi standardok és eljárási szabályok. Például, rendelkezik arról, hogy milyen forrásokból szerezhetők be a munkavállalókra vonatkozó adatok, de nincs utalás a megfigyelés technikájára. Csak az információra és a megállapodásra vonatkozó szabályokat találjuk meg.[82]

A törvény kimondja, hogy a munkáltató ellenőrzési joga nem terjed ki a magáncélú e-mail-ek megfigyelésére és elolvasására. Csak olyan munkáltatói ellenőrzés és megfigyelés lehet jogszerű, amely a munkaviszony zavartalan működése szempontjából szükséges és indokolt. A törvény előírja a munkáltatónak, hogy a munkahelyi elektronikus levelezés megfigyelésére és ellenőrzésére vonatkozó belső szabályzat megalkotása előtt konzultálni kell a munkavállalókkal. Ebben a konzultációs eljárásban a munkáltató kötelessége, hogy a következő paramétereket meghatározza: *a)* a megfigyelés célja, *b)* az alkalmazott módszer és *c)* követendő alapelvek.

A finn „Együttműködésről rendelkező törvény" (Co-operation Act) értelmében a munkahelyen történő megfigyelés bármilyen formájának a bevezetése előtt a munkavállalókat konzultációs jog illeti meg és a munkáltató kötelessége, hogy előre értesítse a munkavállalókat a megfigyelésre vonatkozó döntésének az időpontjáról.[83]

Svédország

A svéd alkotmány 2. és 6. cikkelyei kimondják, hogy az állampolgár leveleit nem nézhetik meg (levéltitok védelme) és a bizalmas kommunikációját semmilyen titkos eszközzel nem rögzíthetik. Ezeket az abszolút jogokat kivételes esetben – külön jogszabályban meghatározott szigorú feltételek fennállása esetén – lehet korlátozni.

A személyes adatok védelméről rendelkező törvény 9. és 10. szakaszai kimondják, hogy a munkavállaló e-mail/Internet forgalmát csak kivételes esetben lehet megfigyelni és ellenőrizni, de ilyenkor is előzetesen figyelmeztetni kell a megfigyelés tényéről. Az „om medbestammande i arbetslivet" jogszabály 11. szakasza kötelezi a munkáltatót, hogy bármilyen a munkavállalók ellenérzését vagy megfigyelését szolgáló rendszer bevezetése előtt köteles előzetesen konzultálni a szakszervezettel.[84]

Norvégia

Norvégiában az Alkotmányon kívül az alapjogszabály a „Személyes adatok védelmére vonatkozó törvény".[85] Ezen kívül az ún. speciális szabályozásként a központi (országos) kollektív szerződésben rendelkeznek a munkahelyi megfigyelésről. Ennek értelmében a

[82] ANDERS VON KOSKULL, 2002, pp. 344–346.

[83] Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final WP 55 Website: www.europa.eu.int/comm./privacy p. 34.

[84] I m. p. 34.

[85] http://www.datatilsynet.no/

rendszer bevezetése előtt a szakszervezetet előre értesíteni kell és a konzultációt kell lefolytatni.

A fenti szikár tényközlésen túl az alábbiakban bemutatunk egy modellt, amelyet azért dolgoztak ki, hogy általa a magánszféra védelmét minél hatékonyabban tudják védeni. A skandináv országokon belül a legszisztematikusabb és legkidolgozottabb – a személyiségi jogok (magánszféra) védelmére vonatkozó – jogelvekkel a norvég „privacy interest model", vagy más zóval a norvég magánszféra jogi védelmének az elmélete (theory of privacy protection – personvern) rendelkezik. A modell lényege a következő: *a)* statikus elem: a rendszer számbaveszi az alapvető emberi jogokat, illetve az ezeket tartalmazó dokumentumokat (pl. Human Rights Convention of the European Council) és *b)* dinamikus elem: egyenként megvizsgálja, hogy a kérdéses magatartás, mulasztás stb. vajon a rögzített emberi jogok keretei közé esik vagy sem. Ennek a megoldásnak az elvi alapja, hogy minden egyes ember magánszféráját megilleti valamilyen szintű jogi védelem.

Ez a „privacy model" döntésorientált (decision orientated). A személyes adatok szolgálnak alapul ahhoz, hogy a munkáltató képes legyen meghozni a döntését. A rendszer lényege, hogy a konkrét szituációktól függően, illetve az adott viszony keretei között mérlegelve hozza meg az arra jogosult a döntését. Az érdekek pontos és körültekintő mérlegelését követően dönthető el, hogy az adott információ milyen viszony, illetve helyzet keretében szolgáltatható ki. Az adott munkavállalóról rendelkezésre álló személyes adat lesz az alapja a vele összefüggésben meghozott döntés alapja.

A modell a különböző egyéni és közérdek érvényesítésére szolgál.

A. Az *egyéni érdekek* leggyakrabban az alábbi három formában jelennek meg: *a)* az információk bizalmas kezelése (confidentiality) – az egyén érdeke ahhoz fűződik, hogy ellenőrizhesse a rá vonatkozó adatok gyűjtését és felhasználását; ugyanakkor ez nem jelent teljes mértékű kontrollt, hanem alapvetően azt kívánja elérni, hogy ne lehessen beleegyezés nélkül adatot gyűjteni és felhasználni; *b)* a döntéshez leginkább megfelelő adat szolgáltatása – adekvátság: ezen belül további két kérdést kell megvizsgálni: *ba)* relevancia (A kért, illetve szolgáltatott információnak az adott kérdés eldöntéséhez relevánsnak kell lennie. A nem releváns adatokat nem lehet kérni, illetve nem kell szolgáltatni. Példálózó jelleggel megemlítünk néhány esetet, amikor nem releváns az adat: már túlságosan elavult, vagy az adott kérdéshez nem kapcsolódik igazán; például a legtöbb esetben a politikai, vallási hovatartozás vagy a nemhez kapcsolódó kérdések irrelevánsak. Ez utóbbi példa jól szemlélteti a személyiségi jogok védelme és a diszkrimináció ellenes jogalkotás közeli kapcsolatát.); *bb)* a megfelelőség (adekvátság) elve, vagyis a szolgáltatott adatnak mindenkor korrektnek kell lennie. Önmagában egy helyesen szolgáltatott adat is lehet nem megfelelő, ha a többi releváns – de a másik fél által nem ismert – tényt nem közöljük. Ezért a megfelelőség (adekvátság) elvét a jóhiszemű együttműködés elvével kell összekapcsolni. *c)* A harmadik egyéni érdek, ami megjelenik: a személyhez kötöttség (access), vagyis a szolgáltatott adat az illető személyre vonatkozzon. Magától értetődik, hogy a fent említett érdekek egymással nagyon szoros összefüggést mutatnak.

B. A *közérdek* megjelenése. *a)* A társadalom tagjaiban megfogalmazódik az igény arra, hogy kontrollálhassák a rájuk irányuló megfigyelés szintjét (controlling the surveillance level in society). *b)* Életerős társadalom létrehozása (robust society). Ez magában foglalja azon gyengeségek kiküszöbölését, amelyek az információs társadalomban – a különböző adatbankok létrehozásakor, vagy hálózatok, illetve információs

sztrádák kiépítésekor – fordulhatnak elő. *c)* A harmadik érdek, egy jóindulatú, jóakaratú igazgatás kiépítése. A privát szférában ennek a megtestesítője a közigazgatás, míg a munka világában ezt az igazgatási funkciót a munkáltató látja el és ezért vele szemben kell törekedni a munkavállalók védelmére.

Mint ahogy azt a magánérdek vonatkozásában jeleztük, a magánérdekekhez hasonlóan a közérdek egyes megtestesítői is egymással szoros kölcsönhatásban vannak, sőt az is bátran kijelenthető, hogy a magánérdek és a közérdek is kölcsönös egymásra hatásban állnak egymással. Ugyanakkor a jogalkotás vagy döntéshozatalkor megfigyelhető, hogy az egyes elvek között ésszerű és kompromisszumra hajló engedményeket kell tenni.

A munkavégzéssel kapcsolatos személyiségi jogok fejlődését vizsgálva megállapítható, hogy ebben meghatározó szerepe van – különösen a skandináv országokban – a kollektív szerződésnek. Történelmileg teljesen nyilvánvaló volt, hogy a munkáltató saját kiváltságának tartotta a munkavégzés feltételeinek – beleértve a kollektív szerződés végrehajtását is – a teljes körű kontrollját. Ez természetesen nem volt ennyire magától értetődő a munkavállalók számára. Ezért e vonatkozásban számos összetűzésre és érdekellentétre került sor. A munkáltatók korlátlan ellenőrzési és megfigyelési jogát is magában a kollektív szerződésben rögzítették. A nagy kérdés természetesen az volt, hogy milyen elvek figyelembe vételével határozzák a határvonalakat: mi az ami még megengedett és mi az ami már nem. Ezt nevezték az „arányos akciók kívánalmának" (requirement of proportionate actions), amely elv az objektíve indokolható megfigyelést tartotta jogszerűnek (reasonable objectives of surveillance). Ugyanakkor sem a jogalkotás, sem a bírói gyakorlat, sem pedig a kollektív szerződéskötési gyakorlat nem feltétlenül ismeri el ezt az elvet: kimondják, hogy a munkáltató megfigyeléshez és az ellenőrzéshez való joga nem legitimizál minden egyes munkáltatói magatartást. Vagyis nem jelenti azt, hogy minden a munkáltató által szükségesnek tartott akció egyidejűleg automatikusan jogszerű is lesz. A következő elvek sietnek a munkavállalók segítségére: *a)* arányos magatartás (proportionate measures); *b)* adekvát magatartás (adequate measures); c) megfelelő munkaerőpiaci standardok, amelyek képesek felvenni a harcot a munkáltatói túlzásokkal szemben (good labour market standards) stb.

Alapvetően a fenti szempontok különböző konstellációja alakítja napjaink magánélet védelmére, illetve ezen belül az adatvédelemre vonatkozó normatív szabályozásának főbb vonalait.[86]

Svájc

1. A munkáltató ellenőrzési joga

Alapvetően a munkáltatónak jogában áll a munkavállalók e-mail/Internet használatát ellenőrizni, de ez az ellenőrzési jog nem korlátlan. A munkáltató ellenőrzési joga a Swiss Code of Obligations (Svájci Kötelmi Kódex) 321d. cikkelyéből ered. Ez a jogszabályhely kimondja, hogy a munkáltatónak joga van a munkavégzésre és a munkahelyi viselkedésre vonatkozó iránymutatásokat és utasításokat adni. A munkavállalónak pedig

[86] ANDERS VON KOSKULL: Employment Privacy Protection – Scandinavian Comparative Perspectives; in. *Stability and Change in Nordic Labour Law*, ed. Peter Wahlgren, Scandinavian Studies in Law Volume 43, Stockholm Institute for Scandinavian Law, Stockholm, 2002, pp. 335–339.

kötelessége, hogy a kapott utasításokat és iránymutatásokat legjobb tudása szerint végrehajtsa, ezáltal is védve a munkáltató jogos gazdasági érdekeit.

1.1. Az ellenőrzés korlátjai

A Code of Obligations 328b. cikkelye és a Svájci Szövetségi Adatvédelmi törvény (Swiss Federal Act on Data Protection), valamint az együttes végrehajtásukra kiadott rendelet (Ordinance) tartalmazza a munkavállalói e-mail/Internet használat munkáltatói ellenőrzésének korlátait. A Code of Obligations 328b. cikkelye kimondja, hogy „a munkáltató csak olyan adatokat kérhet és tarthat nyilván amely a munkavállaló szakmai képességeire utal vagy amelyek a munkaviszonyból származó kötelezettségek teljesítése szempontjából szükséges". A svájci adatvédelmi biztos, aki az Adatvédelmi törvény végrehajtásáért felelős kiadott egy a munkahelyi e-mail/Internet használatára és ennek a munkáltatói ellenőrzésére vonatkozó ajánlást. Az ajánlást mind a közszférában, mind pedig a magánszférában dolgozókra vonatkozik.

Az ajánlás értelmében a munkahelyi e-mail/Internet megfigyelés nem irányulhat szisztematikusan és folyamatosan egy kiválasztott munkavállalóra vagy munkavállalói csoportra. Kivétel, ha alapos gyanú van arra nézve, hogy valamely munkavállaló vagy munkavállalói csoport rendeltetésellenesen használja a munkahelyi e-mail/Internet kommunikációt. Ilyen esetben a munkáltatónak joga van arra, hogy egy konkrét és személyre szabott ellenőrzési mechanizmust felállítson. Az alapos okra példa lehet, ha a munkáltató által végzett általános (nem egyénre szabott vizsgálat, hanem az egész rendszer rutinszerű ellenőrzéséről van szó) e-mail/Internet vizsgálat során kiderül, hogy valamely munkavállaló nem szakmai, sőt illegális célra használta a rendszert.

Amennyiben felmerül az alapos gyanú, akkor a munkáltató által elrendelt egyénre szabott vizsgálatnak a következő kritériumoknak meg kell felelnie:

a) Előzetes értesítés: A munkavállalót előre értesíteni kell az e-mail/Internet ellenőrzésről;

b) Proporcionalitás elve: A vizsgálat módszerének és tartamának összhangban kell lenni a feltételezett jogsértés nagyságával. Minden egyes konkrét esetben külön kell mérlegelni az arányosság – a munkáltató gazdasági érdeke és a munkavállaló magánérdeke – kérdését.

c) Az e-mail/Internet ellenőrzés nem akadályozhatja meg az alapvető emberi (munkavállalói) jogok érvényesülését. Ilyen alapvető jog például a Svájci Alkotmány 13. cikkelyében[87] rögzített a magánszféra védelméhez való jog. Például, nem lehet a munkahelyi levelezési rendszerben küldött magánlevelet közzétenni, még akkor sem, ha a munkahelyen nem engedélyezett a magáncélú levelezés. Magától értetődik, hogy amennyiben felmerül a gyanú, hogy a munkavállaló valamilyen bűncselekményt követett el, akkor a nyomozóhatóságnak – de csak bírósági felhatalmazás beszerzését követően – joga van a magánlevelezés megtekintésére.

Az adatvédelmi biztos ajánlása alapvetően az ILO Általános Irányelvét (General Directive) követi.

[87] A svájci alkotmány 13. cikkelye: „Minden személynek joga van arra, hogy a magán- és családi életét, magánlevelezését és telekommunikációs tevékenységét tiszteletben tartsák. Minden személynek joga van a személyes adatainak a védelméhez."

2. Szankciók és felelősségi kérdések

2.1. Fegyelmi büntetések

A jogellenes munkahelyi e-mail/Internet használat egyik lehetséges szankciója a fegyelmi büntetés. Ennek a meghozatal előtt értesíteni kell a munkavállalót. Hatékony prevenciós eszköz lehet annak a biztosítása, hogy a munkáltató a többi munkavállalónak kihirdetheti – az érintett munkavállaló nevének elhallgatásával - a fegyelmi ügy tényállását és a kiszabott büntetést. Ugyanakkor még egyszer ki kell hangsúlyozni, hogy a munkáltatónak alapvetően nincs joga arra, hogy betekintsen a munkavállaló magánlevelezésébe.

2.2. Kártérítési felelősség és a munkaviszony azonnali hatályú megszüntetése

A svájci Code of Obligations kártérítésre vonatkozó általános szakaszai alapján a munkavállaló a munkaszerződés megszegésével a munkáltatónak okozott mindennemű kárért felelősségre vonható. A súlyos kontraktuális kötelezettségszegés esetén a munkáltatónak joga van a munkaviszony egyoldalú és azonnali hatályú megszüntetésére.

2.3. Büntetőjogi felelősség

A svájci Büntető Törvénykönyv értelmében az e-mail/Internet jogellenes használata – függetlenül attól, hogy azt a munkavállaló vagy a munkáltató végzi - büntetőjogi tényállást valósíthat meg. A munkáltató egy másik Btk-beli tényállás alapján is felelősségre vonható, feltéve ha a munkavállaló e-mail/Internet használatának ellenőrzése során megsérti a Büntető törvénykönyvben szabályozott „a magánszféra védelme" tényállást. Például, ha a munkavállaló beleegyezése nélkül olvassa el a munkavállaló magánlevelét, akkor megsérti a levéltitkot, ezzel pedig bűncselekményt követ el (Svájci Btk. 179. §).

3. Az ellenőrzés technikai módszerei

Alapvető kérdésként merül fel, hogy milyen módon lehet különbséget tenni az e-mail/Internet hivatali, illetve magáncélú alkalmazása között. A munkáltató kötelessége, hogy teljesen pontosan meghatározza a munkahelyi e-mail/Internet használatának a lehetséges eseteit. Mikor és milyen célra használhatja a munkavállaló. Melyek az engedélyezett magáncélú felhasználások és melyek az engedély nélküliek stb. Ezeket az előírásokat egy munkahelyi szabályzatba (kézikönyvbe, utasításba stb.) kell rögzíteni.

Egy másik – technikai – megoldás, amikor a munkáltató létrehoz egy belső honlapot (home-website), amelyik minden esetben bejelentkezik amikor a munkavállaló megnyitja az internetet. Ezen kívül a vírusmentesítés céljára létrehozott ún. tűzfal (firewall) egyidejűleg biztonsági célt is szolgálhat, vagyis nem engedi fel a munkavállalót az eleve tiltott internetes honlapokra, illetve korlátozza az e-mail/Internet használatának az időtartamát.

Az adatvédelmi biztos által a munkáltatók számára adott ajánlások:

a) meg kell határozni, hogy milyen célra lehet használni az internetet, milyen honlapokat lehet, illetve nem lehet megnyitni. Az e-mail/Internet privát célú használatát vagy

teljes egészében megtiltja, vagy csak pontosan meghatározott feltételek mellett – időtartam, cél stb. – engedélyezi;

b) megtiltja bizonyos – pl. tiltott, pornográf, diszkriminatív jellegű stb. – honlapok látogatását;

c) szabályozza a speciális internetes tevékenységeket, mint például az internetes beszélgetés (chat) vagy az információs adatbázishoz (newsgroups) történő csatlakozás. Ezeket az internetes lehetőségeket csak a munkáltató kifejezett engedélyével használhatja;

d) A munkahelyi kommunikációs rendszeren bizonyos – nem kívánatos – magatartások korlátozhatók. Ilyen kifogásolt magatartás lehet például a hirdetési tevékenység, vagy pilótajáték, vagy szándékosan túlságosan nagy file küldése stb.

A munkáltató ugyancsak megtilthatja, hogy a munkavállaló bizonyos inkriminált adatokat lementsen a hálózatról, vagy magáncélú banki vagy értéktőzsdei müveleteket végezzen, vagy internetes vásárlást bonyolítson le stb.

Általános megjegyzésként az az alapszabály állapítható meg, hogy minél inkább tiltani szeretné a munkáltató a munkahelyi e-mail/Internet használatot, annál több és részletesebb – munkahelyen belüli – tiltó vagy megengedő szabályt kell alkotni. Ez pedig egy idő után öncélúvá válhat, illetve azzal a veszéllyel jár, hogy ellehetetlenül az elektronikus médiákon való munkavégzés.

3.1. Szociális párbeszéd

Ellentétben sok európai ország munkajogi gyakorlatától Svájcban nincs a munkavállalóknak állandó és kötelező érdekképviselete a munkahelyeken. Az, hogy egyáltalán vane ilyen szerv az adott munkahelyen és nekik milyen beleszólási jogosultságot biztosítanak a munkáltatói döntésekbe mindig esetleges és a diszkrecionalitás elvén alapul.

Befejezés

Munkánkban az EU tagállamok normaalkotását és joggyakorlatát áttekintve bemutatuk a joggyakorlat oldaláról jelentkező és világosan érzékelhető elvárást, miszerint tisztázni kell, hogy vajon az általános adatvédelmi szabályozási elvek és szabályok alkalmazhatók-e a specifikusnak számító munkavégzési jogviszonyokra vagy az általános elveken alapulva a munkaviszony alanyaira külön speciális normákat kell alkotni. Hasonló kérdésfelvetéssel találkozhatunk más nemzetközi szervezeteknél, akik ezzel a kérdéssel foglalkoznak. Az eddigi tapasztalatok azt mutatják, hogy jelentős igény mutatkozik arra, hogy a „csak" általános érvényű adatvédelmi szabályozáson kívül legyen specifikus – a munkavállalók személyes adatainak és magánszférájának a védelmére szolgáló – szabályozás is. A jelenlegi uralkodó álláspont szerint ezt egy EU-szintű keretmegállapodásban lehetne leginkább megvalósítani. Ennek a lehetséges pontjait szintén bemutattuk.

Ezzel összefüggésben a gyakorlatban az tapasztalható, hogy néhány tagállamban az általános adatvédelmi elveket és szabályokat különféle értelmezések útján igyekeznek a munkavégzésre is alkalmazni. Ez némely esetben előre pontosan nem látható negatív következménnyel – bizonytalanság, ellentmondás stb. – is járhat. Más tagállamokban, ahol már van ugyan külön munkaviszonyban álló személyekre vonatkozó specifikus szabályozás, de ez(ek) normá(k) rendszerint nem átfogóan, hanem fragmentáltan szabá-

lyozzák a kérdéseket. Például néhány tagállamban csak a munkaerő felvétellel kapcsolatos adatvédelmet szabályozzák. Más tagállamokban csak az egészségügyi adatok kezelésére van szabály, de gyakran még ezekben a specifikus normákban sem rendelkeznek például a drogtesztből vagy a genetikai vizsgálatokból származó adatok kezeléséről.

A fenti probléma felvetésén kívül elmondható, hogy a már meglévő EU-s és tagállami szabályok gyakorlati alkalmazása sem mindig problémamentes. Például, a munkáltatók többsége még mindig abban – a mára már megkérdőjelezhető – a téves feltevésben van, hogy a munkavállaló beleegyezése jogszerűvé teszi a munkáltatói intézkedések, ellenőrzések, megfigyelések stb. összességét, még azokat is, amelyek egyébként nyíltan és nyilvánvalóan sértik a munkavállaló személyhez fűződő jogait. Például, sok munkáltató úgy gondolja, hogy amennyiben a munkavállaló beleegyezett akkor – függetlenül a betöltendő vagy betöltött munkakörtől – kérhető a munkavállalótól a rá vonatkozó teljes körű egészségügyi, vagy bűnügyi nyilvántartás, vagy a beleegyezés lehetővé teszi, hogy a munkáltató rutinszerűen és folyamatosan megfigyelje a munkavállaló e-mail/Internet (beleértve a magánjellegű e-mail) forgalmának a tartalmát stb.

A munkavállaló előzetes beleegyezésének a megkövetelése mögött alapvetően két probléma húzódik meg. Egyrészt magában hordozza a munkáltató-munkavállaló eltérő „hatalmi" pozíciójából eredő munkáltatói „akarathajlítás" lehetőségét. Másképpen fogalmazva, a megkérdezéskor a munkavállaló rendszerint nincs abban a helyzetben, hogy nemet mondjon a munkáltatónak. Tehát a beleegyezése formálissá, hiteltelenné, sőt a munkavállaló számára esetleg kierőszakolttá válhat.

Van egy másik pragmatikus probléma. Tételezzük fel, hogy egy multinacionális vállalat minden EU tagállam területén működik 2000–2000 fővel. A jelenlegi tagállamok számát tekintve ez összesen 30.000 munkavállalót jelent. A beleegyezés esetén a munkáltatónak 30.000 darab levelet kell elküldeni. Ugyanennyi nyilatkozatot kell regisztrálni és folyamatosan vezetni a nyilvántartást. Tovább nő az adminisztrációs teher azokban az országokban, ahol a beleegyezésről az Adatvédelmi Hatóságot is tájékoztatni kell.[88]

A formálódó EU-szintű Keretmegállapodás filozófiája szerint ez egyáltalán nem tekinthető általános érvényű elvnek, hanem minden esetben az adott helyzethez kell igazítani a munkáltató lehetőségeit. Jó példaként hozható fel a munkánkban ismertetett Finn Adatvédelmi törvény rendelkezései.

További probléma az adatáramlás szabadságának a megvalósítása. Ez nemzetközi szinten elsősorban az EU és az OECD normaalkotásában jelent meg. A szabályozás fő célja, hogy a globalizált és digitális gazdaság (világtársadalom) időszakában nemcsak az adatvédelmet kell biztosítani, hanem az adatáramlás szabadságát is. Ezt pedig úgy kell megvalósítani, hogy közben az adatalanyok személyiségi jogai és magánszférája ne sérüljön. A XX. század végétől számítva a munkavégzés jellege és struktúrája jelentős mértékben megváltozott. A munkavégző magánélete és az üzleti élete egyre inkább összefonódik. Következésképpen a korábban elfogadott alapvető munkavállalói jogok – például a személyiségi jogok, vagy magánszféra védelme – napjainkban teljesen más értelmezést kapnak. Erre a sajátosságra feltétlenül tekintettel kell lenni az új személyiségi jogi és adatvédelmi szabályozás kialakításakor. A munkavállalók személyiségi jogainak, adatvédelmének szempontjából ugyancsak új értelmezést kap a munkáltató gazdasági érdeke. Az új típusú munkavégzés keretei között már nem lehet a korábban

[88] MORRISON & FOERSTER LLP, August 5, 2002. p. 23.

elfogadott, hagyományos módszereket és eszközöket használni és ugyancsak anakronisztikusnak tűnnek a korábbi célkitűzések. Például, a munkavégzés intenzitását sok esetben nem lehet a korábbi módszerekkel megfigyelni, mert a munkavállaló már nem a munkahelyen, hanem saját otthonában végzi a munkát. A munkáltató egyre inkább a munkavégzés eredményét tudja csak kontrollálni és nem magát a munkavégzés folyamatát. A határokon átáramló adatok miatt sok esetben jogösszeütközésre kerül sor. Eltérő jogrendszerrel és eltérő szintű jogi védelemmel rendelkező országok eltérő szabályait kell alkalmazni. A magánszféra védelmére vonatkozó új jogszabályok megalkotásánál már az új gazdasági viszonyokat és a globalizált adatáramlást is figyelembe kell venni.

A globalizálódó világban termékeként vagy még inkább indukáló motorjaként jelentek meg a multinacionális vállalatok. Ezek nem ismerik az országhatárokat, ezért működésük során egyidejűleg több ország jogát is alkalmazniuk kell. Ehhez a problémához kapcsolódóan számtalan olyan esettel találkozunk az iparilag fejlett országokban – ezek közül is kiemelkedik az USA –, amikor a multinacionális cég székhelyén indítanak keresetet, de maga a vitatott jogi probléma nem ebben az országban, hanem – rendszerint – valamely fejlődő országban fordul elő. Ennek az áthidalására a személyiségi jogok védelme területén egyre többen – elsősorban az USA-ban – szorgalmazzák az ún. multinacionális szintű viselkedési kódex (enterprise-wide Codes of Conduct) kidolgozását. Ez az elgondolás azonban nemcsak egyes multinacionális vállalati vezetők fejében fogalmazódott meg, hiszen az ILO is megalkotta a saját viselkedési kódexét, amellyel segíteni próbálja a viselkedési kódexeken keresztül megvalósuló rugalmas szabályozás elterjedését.

Az elgondolás lényege, hogy a multinacionális vállalatokon belül egy viselkedési kódexben kellene szabályozni az összes adatgyűjtésre, feldolgozásra és áramlásra vonatkozó kérdést. Ez egy pragmatikus megoldási javaslat. Például egy az EU. tagállamaiban működő multinacionális cégnél egy kódex megalkotásával kiküszöbölhető lenne, hogy az összes tagállamban legyen egy-egy (összesen 15 vagy a jövőben még sokkal több) kódex. A multinacionális viselkedési kódex létrehozásával elkerülhető, hogy a vállalaton belül több száz szerződést kelljen nyilvántartani. Ez a megoldás első látásra nagyon szimpatikus, de nézzük meg a mögötte meghúzódó esetleges veszélyeket.

Ez a koncepció megoldhatná a különböző államokban működő vállalatok jogösszeütközésből eredő problémáit. Ez alapvetően egy államok feletti (szupranacionális) szintű, privát (nem állami) jogalkotásnak tekinthető. Privát, mivel a multinacionális vállalatok saját maguk hozzák létre. Jobb esetben a szociális partnerek is közreműködnek a megalkotásban. Szupranacionális, mivel a több tagállamban tevékenykedő cég az egyes államok belső normái fölött lévő normát hoz létre. A multinacionális viselkedési kódex szabályai – az adott vállalat munkavállalóira nézve – rendszerint megelőzik az adott állam nemzeti jogalkotását. Ez természetesen kétélű fegyver. Olyan államokban, ahol nagyon magas szintű a munkavállalók magánszférájának és személyiségi jogainak a védelme visszaesést jelenthet, míg olyan államokban, ahol nagyon alacsony szinten van, vagy egyáltalán nem létezik ilyen jellegű szabályozás, ott minden bizonnyal előrelépést jelent.

Ez a megoldás azonban aggályos lehet az egyenlő bánásmód megvalósítása szempontjából is. Hiszen egy adott államban más standardok – jobbak vagy rosszabbak, ideális helyzetben ugyanolyanok – vonatkoznak majd egy multinacionális cég alkalmazottjaira, mint egy más típusú munkáltatónál munkaviszonyban álló személyre.

További probléma, hogy nincs kialakult mechanizmusa a multinacionális viselkedési kódexek jóváhagyásának (megerősítésének). Sem nemzetközi, sem EU-s, sem pedig tagállami szinten nem létezik egy olyan hatóság vagy szerv, amely az ilyen típusú normákat jóváhagyná. Ezért elhangzott az a felvetés, hogy az EU Bizottságának biztosítani kell, hogy bármely olyan javaslat, amely az adatvédelmi irányelv módosítását célozza egyben magában foglaljon egy olyan előterjesztést is, amely feljogosítja a Bizottságot, hogy saját hatáskörében és gyorsított eljárásban jóváhagyhassa az elé terjesztett multinacionális viselkedési kódexet. Ezen kívül, egy ilyen javaslatnak azt is tartalmaznia kellene, hogy az egyes tagállamok saját maguk is – belső jogszabályaiknak megfelelően – jóváhagyhassák a multinacionális viselkedési kódexet. Az ily módon Közösségi és tagállami (az összes érintett tagállamról szó van) szinten megerősített kódex kölcsönös elismerést és relatív legitimitást vívhatna ki magának az EU-s tagállamokban. Ez a megoldás csökkenthetné a rendszerre nehezedő feszültséget.

További probléma, hogy a viselkedési kódexek megalkotását rendszerint a munkáltatók végzik. Ebből következően elképzelhető, hogy a munkaviszony egyik – rendszerint eleve erősebb pozícióban lévő – alanya alkot meg egy olyan normát, amely utána kötelező lesz a munkaviszony másik – rendszerint kiszolgáltatottabb – alanyára, a munkavállalóra is. A megoldás az lehetne, ha a munkavállalók érdekképviseleti szerveit be lehetne vonni a normaalkotás folyamatába. A további kérdés az, hogy kik lesznek azok a munkavállalói érdekképviseletek, akiket be kell vagy be lehet vonni. Ugyanis a jelenlegi érdekképviseleti szervek – dominánsan szakszervezetek és/vagy üzemi tanácsok – leginkább az egyes államokon belül működnek. Országos, ágazati vagy vállalati szinten szerveződnek és nem multinacionális szinten. Ezért tevékenységi körük csak a saját államukon belüli munkaügyi kapcsolatok alakítására terjed ki, vagy még annál is szűkebb, például csak egy ágazatra vagy egy konkrét munkáltatóra. A létező modell tehát több szempontból sem felel meg a multinacionális viselkedési kódex megalkotásához megkívánt szerepnek.

Álláspontunk szerint egy multinacionális vállalat által létrehozott viselkedési kódex megalkotásánál három alapvető lehetőség van a munkavállalói részvétel biztosítására. *1.* A multinacionális vállalat megkeresi az összes érintett országban működő munkavállalói érdekképviseleti szervezetet és mindegyikkel konzultál. 2. A másik megoldás, ha létrehoznak az adott konkrét multinacionális vállalaton belül működő multinacionális szintű munkavállalói érdekképviseleti szervet. Ez a megoldás alapvetően hasonlít az ún. vállalati érdekképviseleti rendszerhez, azzal az eltéréssel, hogy tevékenysége nem csak egy adott országban működő vállalatra terjed ki a tevékenysége, hanem az országhatárokon átívelő multinacionális érdekképviseleti szervezetet hoz létre. Ennek a gyakorlati megvalósítása nem egyszerű, de az Internet és az elektronikus kommunikáció korában egyre inkább kivitelezhetőnek látszik. A harmadik megoldás, a nemzetközi szintű – a multinacionális vállalatok feletti – munkavállalói érdekképviseleti szervezet(ek) létrehozása. Ennek az lenne a feladata, hogy minden szinten és minden államban képviselje a munkavállalók érdekeit. Ez utóbbi megoldáshoz némileg hasonlít – legalábbis regionális szinten – a már meglévő Európai Üzemi Tanácsi, illetve EU-s szintű szakszervezeti érdekképviseleti rendszer. A létező példák ellenére úgy tűnik, hogy a nemzetközi szintű érdekvédelmi szervezet gyakorlati kivitelezhetősége és hatékonysága a leginkább kérdéses. Álláspontunk szerint leginkább a második modell látszik a leginkább kivitelezhetőnek.

Azt is meg kell jegyeznünk, hogy a multinacionális szintű érdekegyeztetés kérdése nemcsak gazdasági kérdés, hanem nagyon fontos kulturális, politikai dimenziói is vannak. Egészen más a tárgyalási alap, a módszer az eljárás például a General Electric Multinacionális cég USA-beli központjában, az USA-beli munkavállalókkal, vagy Budapesten vagy Kínában a helyi munkavállalókkal. A belső normaalkotás során ezt a gazdasági, kulturális, politikai sokszínűséget (multikultúrális munkavállalói érdekképviselet, illetve multikulturális szociális partnerség) kellene összehangolni. Meggyőződésem, hogy – főleg a kezdeti időszakban – nem lehet teljesen azonos multinacionális standardokat alkotni, hanem csak egy közös, minimum standard megalkotását lehet reális célként kitűzni. Később, ennek elérését követően lehetőséget kell biztosítani az egyes államokban működő leányvállalatoknak, hogy az általánosan elfogadott és már elért minimum standardokon kívül a saját körülményeiknek leginkább megfelelő speciális szabályokat hozzanak létre és alkalmazzák azokat. Ugyanakkor, nagyon fontos megszorításként kell érvényesíteni, hogy a speciális szabályok és elvek nem lehetnek ellentétesek az általános standardok „szellemével".

Újabb probléma az ún. atipikus munkavégzők személyiségi jogainak és magánszférájának a védelme. Közüllük is kiemelkednek az elektronikus úton, elektronikus kommunikációs eszközök segítségével munkát végzők. Náluk ugyanis nagyon sokszor – fizikai értelemben is – összeolvad a munkahely és a lakóhely (privát szféra). A számítógép ugyanabban a lakásban van, ahol a mindennapi életük is zajlik. A lakás tehát egyidejűleg lesz lakótér és munkahely. Ilyen esetben nagyon nehéz elhatárolni a magán- és a közszférát. A személyiségi jogok védelme szempontjából pedig ez – legalábbis az uralkodó álláspontoknak megfelelően – elengedhetetlenül fontos. Esetükben az ún. individualizált feltétel- és eredményorientált munkavégzés meghonosítása látszik a megoldásnak. Ez sokkal inkább hasonlít egy tipikus magánjogi jogviszonyhoz (pl. vállalkozás vagy megbízás), mint munkaviszonyhoz. A munkavállalónak kell biztosítani a jogszabályokban meghatározott standardoknak megfelelő munkavégzési helyet és munkakörülményeket. Rendszerint a munka megszerzése érdekében lefolytatott versenyeztetést (munkaszerzésre irányuló tender) követően a munkáltató adja a munkát és pontosan meghatározza a munka elvégzéséhez elengedhetetlenül szükséges mennyiségi, minőségi és ütemezési instrukciókat. Ugyanakkor a munkavégzés során a munkáltató általában nem kíséri – sőt nem is kísérheti, mert nincs abban a helyzetben – folyamatosan nyomon a munkafolyamatot és nem ad rendszeresen utasításokat a munkavállalónak. A munkáltató csak a kiadott utasításoknak megfelelő vagy meg nem felelő munkavégzés eredményét fogja csak látni. Ez alapján fogja megfizetni a munkavállaló munkabérét.

A munkáltatónak ilyen esetben is feltétlenül be kell tartani az adott munkavégző személy államában lévő és – a legutóbbi, főleg USA-beli bírói gyakorlatnak megfelelően – a saját anyaországában rá nézve irányadó munkajogi normákat. A munkavégzés ilyen formában történő individualizálása a munkáltatótól is egyéni bánásmódot kíván. Minden pillanatban pontosan tudnia kell, hogy mennyi munkát adhat, mikor haladja meg a munkavégzés a rendes munkaidőt, mikor válik szükségessé az éjszaka történő munkavégzés, tisztában kell lennie a diszkriminációra vonatkozó tilalmakkal és a konkrét munkavégző személy családi helyzetével stb. A másik oldalon pedig a munkavállalótól is nagyfokú és korrekt együttműködés követelhető meg: pontosan nyilván kell tartania, hogy hány órát dolgozott, szüksége volt-e az éjszakai munkavégzésre, vagy el tudta volna végezni a munkát nappal is, ha napközben nem megy el inkább úszni stb.

Ebben az új típusú munkavégzési viszonyrendszerben a munkavállaló személyiségi jogai éppen úgy védelemre szorulnak, mint a hagyományos munkaviszony keretében munkát végző személyé. Sőt, bizonyos értelemben az atipikus munkát végző munkavállaló még jobban kiszolgáltatott. A munkavállalónak egyre több információt kell szolgáltatnia magáról és a munkavégzésről. Ez pedig magában hordozza annak a veszélyét, hogy visszaélhetnek ezekkel az információkkal.

További probléma az elektronikus munkát végző személyekkel, hogy ők rendszerint nem csak egy adott munkáltatóval állnak – és rendszerint nem is csak egy országban – jogviszonyban. Az adott személy az egyik órában még az egyik munkáltatónak X. országban végez munkát, de a következő órában már egy másik országbeli vagy akár ugyanabból az országból származó, de másik cég számára végez munkát, és így tovább. Ilyen esetben a lex loci laboris elvének egy új értelmezését kell bevezetni. Ennek értelmében a munkavállalóra legalább a munkavégzés helyén érvényes munkajogi és munkavédelmi standardok érvényesek. Ettől a felek kölcsönös megegyezéssel – pozitív irányban – eltérhetnek. Természetesen ez a megoldás magában rejti a szociális dömping veszélyét. Éppen ennek elkerülése érdekében rajzolódik ki az a gyakorlat – elsősorban az USA-ban lehet megfigyelni –, hogy a munkáltató a saját anyaországában is perelhető, az amerikai szabályok alapján a más – rendszerint jóval elmaradottabb országban tanúsított magatartásáért. Amennyiben ez a gyakorlat általánossá válik, akkor némileg csökkenthető lenne a globalizált piac által intenzíven ösztönzött szociális dömping. Ezen kívül azzal a problémával is számolni kell, hogy az adott országban nincs semmiféle szabályozás az adott kérdésben. Ilyenkor lesz szerepe a nemzetközi standardoknak, illetve a szociális klauzuláknak.

Ebben az átalakuló, egyre inkább globalizálódó világban az egyén (de méginkább, a munkavállaló) kiszolgáltatottsága sok vonatkozásban maximális. Ezért mindenféle megkülönböztetés nélkül, alapértékként kell védeni a munkavállaló emberi méltóságát és alapvető szabadságjogait. Álláspontom szerint ennek az értéknek minden más gazdasági szemponttal szemben prioritást kellene élveznie.

Függelék

1. sz. függelék (az I. részhez)

A szociális partnerek álláspontjai a 95/46/EC irányelv módosításának egyes kérdéseiről

a) Munkavállalói beleegyezés

UEAPME: Nincs szükség további formális kívánalmakra. A szerződő felek közötti kapcsolatnak a bizalmon kell alapulnia.

ETUC: A beleegyezés megkövetelése nem ad megfelelő védelmet a gyengébb pozícióban lévő munkavállaló számára.

CEC: Álláspontja szerint létre kell hozni a személyes adatok egy olyan katalógusát, amelyhez a munkáltató, még a munkavállaló beleegyezése esetén sem férhet hozzá.

EUROCADRES: A beleegyezés nem teheti legitimmé az adatfeldolgozást.

b) Egészségügyi adatok

UNICE: Ezzel a kérdéssel a Munkahelyi Egészség és Biztonságról rendelkező irányelvek foglalkoznak.

UEAPME: A 95/46/EC irányelv 6. Cikkelye releváns. További jogszabályalkotás tagállami szinten kívánatos.

ETUC: A munkáltatót csak annyiban érdekelhetik az egészségügyi adatok, hogy megállapíthassa, vajon a munkavállaló alkalmas-e az adott munkakör betöltésére. A munkáltató által további egészségügyi adatok megszerzése indokolatlan.

EUROCADRES: Az ilyen adatok feldolgozása és kezelése nagy körültekintést kíván. Ennek az oka: *a)* az adatok érzékenysége és *b)* magában hordozza a diszkrimináció lehetőségét.

c) Drog-teszt

UNICE: Az ilyen jellegű adatok feldolgozása akkor jogszerű, ha munkabiztonsági okból teszik.

UEAPME: A 95/46/EC irányelv 6. Cikkelye releváns. További jogszabályalkotás tagállami szinten kívánatos..

ETUC: Nincs szükség kötelező és általános jellegű drog tesztre.

EUROCADRES: Az ilyen adatok feldolgozása és kezelése nagy körültekintést kíván. Ennek az oka: *a)* az adatok érzékenysége és *b)* a magában hordozza a diszkrimináció lehetőségét.

d) Genetikai adatok

UNICE: A tudomány gyors fejlődése miatt a szabályozás tagállami szinten lehet leginkább megfelelő.

UEAPME: A 95/46/EC irányelv 6. Cikkelye releváns. További jogszabályalkotás tagállami szinten kívánatos.

ETUC: A munkaviszony létesítését megelőző genetikai teszt teljes körű tiltását szorgalmazza. A munkáltató önkéntes döntése alapján kezdeményezhet alapszintű és ellenőrzött genetikai tesztet. Az ellenőrzés lehetősége széles körű, de például az érintett munkavállaló kontrollálhatja a tesztet.

EUROCADRES: A genetikai teszt eredményén alapuló diszkrimináció szigorú tilalmát szorgalmazza.

d) Megfigyelés és ellenőrzés

UNICE: Van legális alapja a munkavállaló megfigyelésének és ellenőrzésének. Mind nemzetközi, mind pedig tagállami szinten léteznek olyan módszerek és technikák, amelyek jogilag megfelelők.

UEAPME: A téma eltér a fentiekben tárgyalt kérdésektől. A kérdés rendezésének alapvető szintje a vállalati szintű kollektív szerződés.

ETUC: A folyamatos és automatikus ellenőrzés betiltását javasolja. Különösen az olyanokat, amelyek azonnali adatgyűjtésen (real time) alapulnak és amelyről előre nem informálják a munkavállalót.

CEC: Alapvetően ellenzi a munkavállalók e-mail/Internet forgalmának a megfigyelését. Kivételt csak abban az esetben lehet tenni, ha az különösen indokolt. Támogatja egy olyan munkahelyi szabályzat (company's code) megalkotását, ahol részletesen rendezik a magáncélú e-mail/Internet használatot.

EUROCADRES: Különös figyelmet szentel ennek a kérdésnek. Tiszta szabályok megalkotását szorgalmazza. Visszautasítja annak a lehetőségét, hogy a munkavállaló beleegyezése legitimálja a munkáltatói megfigyelést. Tekintettel az ILO 1996-os Code of Practice-ra és az Európa Tanács R (89) 2 Ajánlására azon az álláspontón van, hogy ebben a kérdésben a munkáltatónak, munkavállalóknak és munkáltatói érdekképviseleti szerveknek együtt kell működniük.[89]

[89] http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf; Second stage consultation of social partners on the protection of worker's personal data, p. 19–20.

2. számú függelék (a II. részhez)

Összefoglaló táblázat az EU és EGT tagállamok jogi szabályozásáról

Ausztria
– Alapjogszabály: Személyes adatok védelmére vonatkozó szövetségi jog (datenschutz)[90]
– Speciális szabály vonatkozik az ún. érzékeny adatok munkahelyen történő felhasználásáról[91]
– A munkahelyi megfigyelést illetve ellenérzést szolgáló rendszerek bevezetése előtt a szociális partnereket (leginkább üzemi tanács) előzetesen értesíteni kell, akiknek egyetértési joguk van.[92]
– A munkavállalók és a munkára jelentkezők genetikai teszttel történő vizsgálata tilos.
Belgium
– Alapjogszabály: A magánszemélyek személyiségi jogának védelméről rendelkező szövetségi szintű törvény (1992. december 8.)[93]
– Speciális szabály vonatkozik a munkavállalók egészségügyi vizsgálatából származó egészségügyi adatok kezelésére.
– Regionális szinten külön rendelet foglalkozik a munkaerő kiszerződésére (outplacement), munkaerő felvételre és a munkaerő közvetítésre vonatkozó érzékeny adatok kezelésével.
–Két kollektív szerződés (No. 13 és No. 68) tartalmaz szabályozást a szociális partnerek informálására és a velük folytatandó konzultációs eljárásra.
Dánia
– Alapjogszabály: A személyes adatok feldolgozásáról rendelkező törvény (Act No. 429, 2000. május 31.)[94]
– Speciális szabályozás: a munkavállalók egészségügyi vizsgálatából származó egészségügyi adatok kezelésére.
– Külön speciális szabályozás vonatkozik az állami (közszolgálati) alkalmazottakra.
Finnország
– Alapjogszabály: Személyes adatokról rendelkező törvény (523/1999)[95]
– Speciális szabályozás: a magánszféra védelme a munkavégzés során. A törvényt a finn Parlament 2001. májusában fogadta el.[96]

[90] http://www.bka.gv.at/datenschutz/indexe.htm

[91] Az adatvédelmi törvény 9. szakasz 11. bekezdése.

[92] Constitutional Act on Labour No. 22/1974, 96. szakasz.

[93] http://www.privacy.fgov.be/loi98coordi.htm

[94] http://www.datatilsynet.dk/eng/index.html

[95] http://www.tietosuoja.fi/hopxtvf.HTM

[96] Ez volt az első olyan szabályozás az EU-ban, amely speciálisan a munkavégző személyek adatvédelméről rendelkezett. A törvény a modern személyiségi jogi törvényhozás megtestesítője. Magában foglalja az összes olyan témakört és eljárási megoldást, amely a legkorszerűbb szabályozással szemben elvárható: munkaerő-felvételnél alkalmazható tesztek, kérdések stb. (5. szakasz), egészségügyi és egyéb munkavégzéssel összefüggő tesztvizsgálatok (6. szakasz), genetikai vizsgálat (7. szakasz), a munkavállalók egészségi állapotára vonatkozó adatok (8. szakasz), a munkahelyi e-mail/Internet megfigyelésre és ellenőrzésre vonatkozó előírások (9. szakasz).

Franciaország
– Alapjogszabály: Az egyének magánszférájának védelméről rendelkező 78-17. számú törvény (1978. január 6.) – Speciális szabályozás: A munka törvénykönyvében található speciális szabályozás a munkavállalók személyes adatainak a védelmére.[97]
Németország
– Alapjogszabály: Szövetségi Adatvédelmi törvény (BDSG).[98] – Speciális szabályozás: Közszolgálatban dolgozók számára külön adatvédelmi törvény létezik. [Framework Civil Service Act BRRG-, 56–56f szakaszok; Federal Civil Service Act – BBG-90-90g; (1970)] A törvény kimondja, hogy a munkavállalók megfigyelésére alkalmas technikai eszközök bevezetése előtt az üzemi tanács egyetértését meg kell szerezni. Ez a szabály mind a magán-, mind pedig a közszférában alkalmazandó.
Görögország
– Alapjogszabály: A 2472/97. sz. törvény Az egyén magánszférájának védelme a személyes adatok feldolgozásával kapcsolatos eljárás során (General law 2472/97 on the protection of individuals with respect to the processing of personal data.)[99]
Írország
– Alapjogszabály: Adatvédelmi törvény (1988)[100] – Speciális szabályozás: -
Olaszország
– Alapjogszabály: 675. számú törvény az egyének személyes adatainak a védelméről (1996. december 31.)[101] – Speciális szabályozás: 135. számú törvény az érzékeny adatok kezeléséről a Közigazgatásban (1999. május 11.) – Speciális szabályok tiltják a munkavállalók megfigyelését és ellenőrzését – Az olasz Adatvédelmi Hatóság jogosult engedélyezni az ilyen ellenőrzést vagy megfigyelést (Authorisation No. 2/2000)
Luxemburg
– Alapjogszabály: Az adatok elektronikus továbbításáról rendelkező törvény (1979. március 31.)
Hollandia
– Alapjogszabály: Alkotmány és az Adatvédelmi törvény (2000. július 6., amely 2001. szeptember 1-én lépett hatályba) – Speciális szabályozás: Munkajogi szabályok az üzemi tanács tájékoztatáshoz való és

[97] http://www.legifrance.gouv.fr/html/frame_codes1.htm
[98] http://www.bfd.bund.de/information/BDSG_neu.pdf
[99] http://www.dpa.gr/2472.htm
[100] http://www.dataprivacy.ie/6ai.htm
[101] http://www.astra.garanteprivacy.it/garante/frontdoor/1.1003..00.html

egyetértési jogáról. (Working Conditions Act, 5.1–5.3. szakaszok (1998. november); Üzemi Tanácsról rendelkező törvény (1999. október); Kormányzati tisztviselők munkajogi szabályozásáról szóló törvény (2000. december.)
- A munkavállalók fizetési jegyzékéről és betegségi nyilvántartásáról rendelkező törvény. A törvény 29. szakasza kimondja, hogy amennyiben van kollektív szerződés, akkor az ilyen tárgyú kérdésekről a szakszervezeteket informálni kell, velük konzultációt kell folytatni és bizonyos esetekben egyetértési joguk van.
- A munkavállalók etnikai eredetének nyilvántartásáról rendelkező törvény (1998. április). A személyi azonosításról rendelkező [Identification Act (1993. december)] és a Személyi számról rendelkező törvény (2001. január). Amikor jogszabályi kötelezettség előírja, akkor a munkáltató jogszerűen használhatja a munkavállaló személyi számát.

Portugália

- Alapjogszabály: 67/98. számú törvény (1998. október 26.)[102]
- Szektorális szabályozás:
- A Portugál Alkotmány 32. szakasz (8) bekezdés: Bármilyen bizonyíték, amely a magánélet, családi élet, levelezés, egyéb kommunikáció védelmére vonatkozó normák megszegésével kerül beszerzésre érvénytelen és semmilyen eljárásban nem használható fel. A 34. szakasz (1) bekezdése: A magánlevelezés és más magánjellegű kommunikáció sérthetetlen.
- A személyiségi jogok védelmét a telekommunikációs szektorban szabályozó törvény 5. szakasza (69/89. számú törvény, 1998. október 28.)
- Az 5/94. számú rendelet, amely a munkáltató tájékoztatási kötelezettségét írja elő munkaszerződés tartalmára és a munkaviszony feltételeire vonatkozó adatokról a munkavállalók felé. (1994. január 11.)
- A szakszervezeti tagdíj befizetésének rendszerére vonatkozó törvény (81/2001. számú törvény, 2001. augusztus 5.) (3. és 4. szakaszok)
- A munkahelyi egészség és biztonság megteremtését végző szervezetről és működéséről rendelkező rendelet (Decree No. 26/94, 1994. február 1.)

Spanyolország

- Alapjogszabály: A 15/99.számú törvény a személyes adatok védelméről. (1999. december 13.)[103]
- Speciális szabályozás: 994/1999 Királyi rendelet a személyes adatokat tartalmazó számítógépes file-ok kötelező védelméről.[104]
- 1/1995 Királyi rendelet a Law of Statute of Worker végrehajtásáról.[105]
- A 11/1985. számú törvény a Szakszervezeti Szervezkedés Szabadságáról.[106]
- A 31/1995. számú törvény A munkahelyi veszélyek megelőzéséről.[107]

[102] http://cndp.pt/Leis/leis.htm
[103] http://www.agenciaprotecciondatos.org/datd1.htm
[104] http://www.agenciaprotecciondatos.org/datd8.htm
[105] http://www.ccoo.es/legislacion/ley11_8S.htm
[106] http://www.ccoo.es/legislacion
[107] http://websindical.com/legis/prl.htm

Svédország
– Alapjogszabály: A 204/1998. számú törvény A személyes adatokról (1998. október 24.)[108]
– Speciális szabályozás: A szociális partnerekkel köteles konzultálni a munkáltató, ha a munkavállalók megfigyelésére vagy ellenőrzésére szolgáló rendszert – beleértve a videokamerát is – akar bevezetni. A munkavállalók munkateljesítményét csak úgy lehet megfigyelni, illetve ellenőrizni, ha erről előzetesen a munkavállalót értesítik és a szakszervezettel konzultálnak.
Egyesült Királyság
– Alapjogszabály: Adatvédelmi törvény (1998).[109]

Az Európai Gazdasági Térség államai

Norvégia
– Alapjogszabály: Személyes adatok védelmére vonatkozó törvény.[110]
– Speciális szabályozás: A központi (országos) kollektív szerződésben rendelkeznek a munkahelyi megfigyelésről. Ennek értelmében a rendszer bevezetése előtt a szakszervezetet előre értesíteni kell és a konzultációt kell lefolytatni.
Izland
–Alapjogszabály: A 77/2000. sz. törvény Az egyének védelméről a személyes adataiknak feldolgozása során.[111]

[108] http://www.datainspektionen.se/in_english/
[109] http://www.wood.ccta.gov.uk/dpr/dpdoc.nsf
[110] http://www.datatilsynet.no/
[111] http://www.personuvernd.is/tolvunefnd/nsf/pages/

Felhasznált irodalom

- BEDDARD, DR. RALPH: *Human Rights and Europe*. Third Edition, Cambridge, Grotius Publications Limited, 1993.
- *Berkeley Journal of Employment and Labor Law*, Vol.17(1), 1996., Vol.19(1), 1998.
- BOWERS, JOHN: *Employment Law*. Blackstone Press Limited, 1997.
- BREARLEY, KATE: *Employment Covenants and Confidential Information: Law, Practice and Technique*. London, 1993.
- *Condition of work digest. Telework*. Volume 9, No. 1, ILO, Geneva, 1990.
- *Condition of work digest. Worker's privacy Part I: Protection of personal data*. Volume 10, No. 2, ILO, Geneva, 1991.
- *Condition of work digest, Worker's privacy Part II: Monitoring and surveillance in the workplace*. Volume 12, No. 1, ILO, Geneva, 1993.
- *Condition of work digest Worker's privacy Part III: Testing in the workplace*. Volume 12, No. 2, ILO, Geneva, 1993.
- DOHERTY, ROBERT E.: *Industrial and Labor Relations Terms*: a Glossary ILR Press. New York State School of Industrial and Labor Relations Cornell University, Ithaca, NY 1979., 1989.
- DUSTON,ROBERT L.; RUSSEL, KAREN S.; SHEPARD, MICHAEL: *Workplace Privacy*. Washington D.C.,1989.
- *Employee Relations*. Law Journal Vol. 24(1), Summer 1998., Vol.24(3) Winter 1998.
- *European Journal of Law and Economics*. Kluwer Academic Publishers, 1999.
- *European Union Review*. IDS Employment Europe 458 Febr. 2000.
- FINKIN, W. MATTHEW: *Privacy in Employment Law*. BNA Books, The Bureau of National Affairs, Inc., Washington, D.C., USA, 1996.
- FINKIN, MATTHEW W.: *Privacy in Employment Law*. Washington, D.C., Bulletin 68, ILR Press, 1993. New York State School of Industrial and Labor Relations Cornell University
- GOLD, MICHAEL, EVAN: *An Introduction to the Law of Employment Discrimination ILR*.
- HAYDEN, TRUDY; HENDRIKS, EVAN; NOVIK, JACK D.: *Your Right to Privacy*. Southern Illinois Univ. Press, Carbondale, 1990.
- *IDS Employment Europe*. 457 January 2000.
- International Encyclopedia of Comparative Law Volume XV. Chapter 15, 1997.
- *Journal of Individual Employment Rights*. Vol.5(3) 235–249, 1996–97., Vol.6(2) 103–117, 1997–98., Vol.6(3) 179–191, 1997–98., Vol.6(3) 193–199, 1997–98., Vol.7(3) 215–226, 1998–99., 8(2) 125–142, 1999–2000.
- *Legal Issues of European Intergration*. 1996/1, Kluwer Law International.
- *Legal issues of European integration*. 1992/1, Kluwer Law and Taxation Publishers
- MCWHIRTER, DARIEN A.: *Your Rights at Work* c. Könyvből részlet (The Rights to Privacy), John Wiley and Sons, Inc., 1993.
- MICHAEL SHEPARD – ROBERT L. DUSTON – KAREN S. RUSSELL: *Workplace Privacy; Employee testing, surveillance, wrongful discharge and other areas of vulnerability*. The Bureau of National Affairs, Inc. Washington DC. 1989.
- NEAL, ALAN C.: *European Labour Law and Social Policy*. (Cases and Materials) Kluwer Law International, 1999.

- PALMER, CAMILLA: *Discrimination at Work – the Law on Sex and Race Discrimination*. Second edition, Legal Action Group, 1992.
- RANDALL, NICHOLAS; SMITH, IAN: *A Guide to the Employment Relations Act 1999*. London, 1999.
- *The Labor Lawyer* 107, 1997.
- *Transfer European Review of Labour and Research*. Vol. 1–2. Spring-Summer, 1999., Vol. 5(3) Autumn, 1999.
- WACKS, RAYMOND: *Personal Information, Privacy and the Law*. Oxford,1989.
- WAHLGREN, PETER ed.: *Stability and Change in Nordic Labour Law*; Scandinavian Studies in Law, Volume 43; Stockholm Institute for Scandinavian Law, Stockholm 2002
- WHINCUP, MICHAEL: *Modern Employment Law – A Guide to Job Security and Safety*. Ninth edition Butterworth and Heinemann, 1997.
- WRIGHT, BECKY A.: *Employee Benefit Plans: A Glossary of Terms*. Brookfield, Wisconsin 1984.

JÓZSEF HAJDÚ

THE PROTECTION OF WORKER'S DATA PRIVACY, WITH SPECIAL ATTENTION TO ELECTRONIC COMMUNICATION IN THE LEGISLATION OF EU AND ITS MEMBER STATES

(Summary)

Privacy has become one of the most important human rights issues of the modern age. At a time when computer based technology gives government and private sector organisations the ability to conduct mass surveillance of populations, privacy has become a crucial safeguard for individual rights. According to opinion polls, concern over privacy violation is now greater than at any time in recent history. Uniformally, populations throughout the world report their distress about encroachment on privacy, prompting an unprecedented number of nations to pass laws which specifically protect the privacy of their citizens.

The basis for this legal activity rests on a growing understanding that privacy is a fundamental right. Privacy is a process which underpins human dignity and other key values such as freedom of association and freedom of speech. These rights are established squarely in international covenents, and protected specifically in the constitutions of many nations. The increasing sophication of information technology, with its capacity to collect, analyse and disseminate information on individuals, has introduced a sense of urgency to the demand for legislation.

New developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual. Computers linked together by high speed

networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system.

As the pages of this report make clear, rapid advances in the development of powerful technology, in conjunction with the demand for greater management efficiency, are promoting a seamless web of surveillance throughout the workplace. At the same time, inadequate laws and regulations are failing to check an expanding pattern of abuses.

Employees in nearly all sectors are vulnerable to comprehensive surveillance by managers. Legal protections are generally lax in such circumstances because surveillance is frequently imposed as a condition of employment. The changing structure and nature of the workplace has facilitated an increasing level of surveillance.

The technology being used to monitor employees is extremely powerful, and extends to every aspect of a workers life. Miniature cameras monitor behaviour. "Smart" ID badges track an employees movement around a building. Telephone Management Systems (TMS) analyse the pattern of telephone use and the destination of calls. Psychological tests general intelligence tests, aptitude tests, performance tests, vocational interest tests, personality tests and honesty tests – many of which are electronically assessed – raise a great many issues of privacy, control and fairness. Surveillance and monitoring have become design components of modern information systems and the modern work environment.

The use of this technology is often justified on the grounds of health and safety, customer relations or legal obligation. The real purpose of most surveillance, however, is for performance monitoring, personnel surveillance, or outright discrimination. Even in workplaces staffed by highly skilled information technology specialists, bosses demand the right to spy on every detail of a worker's performance. Modern networked systems can interrogate computers to determine which software in being run, how often, and in what manner. A comprehensive audit trail gives managers a profile of each user, and a panorama of how the workers are interacting with their machines.

In this article we deal with the basic questions and legal norms of employees' data privacy at the level of European Union and its member states.

TARTALOM

I. rész

II. rész

A munkavállalók elektronikus kommunikációjához kapcsolódó személyes adatok a védelme az EU tagállamok és az Európai Gazdasági Térség államainak a jogában